目　　录

第一章　整数的整除性

§1. 因数和倍数

我们把 $1, 2, 3, 4, \cdots, n, \cdots$ 这些数叫做正整数，又叫做自然数，其中 $1, 3, 5, 7, \cdots$ 叫做奇数；$2, 4, 6, 8, \cdots$ 叫做偶数.在正整数范围内，很明显，

$$\text{正整数} + \text{正整数} = \text{正整数};$$
$$\text{正整数} \times \text{正整数} = \text{正整数}.$$

但是由正整数减去正整数，得到的可能是正整数，也可能不是正整数。

$$-1, -2, -3, -4, \cdots, -n, \cdots$$

这些数叫做负整数. 而正整数和负整数再加上零，就统一叫做整数。

在整数范围内，我们有

$$\text{整数} + \text{整数} = \text{整数};$$
$$\text{整数} - \text{整数} = \text{整数};$$
$$\text{整数} \times \text{整数} = \text{整数}.$$

但是整数除整数不一定得整数，究竟什么样的整数除什么样的整数才能得整数呢？ 研究这个问题，就是研究整数的整除性。

以后，如果没有特别声明，我们将用

$$a, b, c, d, \cdots$$

等英文字母表示整数. 当几个字母写在一起时，表示将这几个字母相乘起来. 例如

$$ab = a \times b, \quad abc = a \times b \times c,$$

$$abcd = a \times b \times c \times d$$

等. 但注意数目字写在一起时不表示相乘,例如 55 不是 5×5 而是五十五, 234 不是 $2 \times 3 \times 4$ 而是二百三十四. 而当数目字和字母写在一起时,则表示这个数目字和字母相乘.例如 $2a = 2 \times a$, $15a = 15 \times a$, $99abc = 99 \times a \times b \times c$, $1234abcd = 1234 \times a \times b \times c \times d$.

我们还使用记号 $(-a)$ 来表示 $-a$, 即 $(-a) = -a$, 又有 $(-a)(-b) = (-a) \times (-b)$, $(-a)b = (-a) \times b$, $a(-b) = a \times (-b)$.

定义 1 设 a, b 是整数, $b \neq 0$. 如果有一个整数 c, 它使得 $a = bc$, 则 a 叫做 b 的倍数, b 叫做 a 的因数. 我们有时说, b 能整除 a 或 a 能被 b 整除;也有时说, b 能除尽 a, 或 a 能被 b 除尽.

如果 b 能整除 a, 我们就用 $b|a$ 这个符号来表示它,例如 $2|4$, $3|6$. 由于 $-30 = 6 \times (-5)$, $20 = (-5) \times (-4)$, 所以 $6|(-30)$, $(-5)|20$.

如果 b 不能整除 a, 我们就写作 $b \nmid a$, 例如 $2 \nmid 3$, $3 \nmid 8$, $(-3) \nmid 5$, $(-5) \nmid 12$.

如果 a 是一个整数, $a \neq 0$, 而 m 是一个正整数, 则由于 $0 = a \times 0$, $ma = a \times m$, $-ma = a \times (-m)$, 所以 0, ma 和 $-ma$ 都是 a 的倍数. 即

$$0, a, 2a, 3a, 4a, \cdots$$

都是 a 的倍数,而

$$-a, -2a, -3a, -4a, \cdots$$

也都是 a 的倍数. 我们使用记号 $|a|$ 来表示

$$|a| = \begin{cases} a, & \text{当 } a \geqslant 0; \\ -a, & \text{当 } a < 0. \end{cases}$$

我们把 $|a|$ 叫做 a 的绝对值, 例如 $|2| = |-2| = 2$, $|5| =$

$|-5| = 5$.

引理 1 如果 a, b 是二个整数而 $a|b$, 则

$$(-a)|b, \quad a|(-b), \quad (-a)|(-b), \quad |a|\,|\,|b|.$$

证 因为 $a|b$, 所以由定义 1 有一个整数 c, 它使得 $b = ac$, 故得

$$b = (-a)(-c), \quad -b = a(-c) = (-a)c,$$
$$|b| = |ac| = |a|\,|c|.$$

由于 a, b, c, $-a$, $-b$, $-c$, $|a|$, $|b|$ 和 $|c|$ 都是整数, 所以有

$$(-a)|b, \quad a|(-b), \quad (-a)|(-b), \quad |a|\,|\,|b|.$$

引理 2 如果 a, b, c 都是整数而 $a|b$, $b|c$, 则有 $a|c$.

证 因为 $a|b$, 所以由定义 1 有一个整数 d, 它使得 $b = ad$. 又由于 $b|c$, 所以有一个整数 e 它使得 $c = be$. 由 $c = be$ 和 $b = ad$ 有 $c = ade$. 由于 d 和 e 都是整数, 所以 de 也是整数. 由定义 1 和 $c = ade$ 有 $a|c$.

引理 3 如果 a, b 都是整数而 $|a| < |b|$, $|b|\,|\,|a|$, 则有

$$a = 0.$$

证 因为 $|b|\,|\,|a|$, 所以由定义 1 有一个整数 c,它使得 $|a| = |b|c$. 如果 $|a| = 0$, 则有 $a = 0$. 如果 $|a| > 0$, 则由 $0 < |a| < |b|$ 和 $|a| = |b|c$ 有 $c \geqslant 0$. 如果 $c > 0$, 则由于 c 是整数而有 $c \geqslant 1$. 由 $|a| = |b|c$ 和 $c \geqslant 1$ 有 $|a| \geqslant |b|$, 这和 $|a| < |b|$ 发生矛盾, 所以有 $c = 0$. 由 $c = 0$ 和 $|a| = |b|c$ 有 $a = 0$.

引理 4 如果 a, b 是二个整数, $b \neq 0$, 则一定有并且只有二个整数 q, r, 可使

$$a = bq + r, \quad 0 \leqslant r < |b|$$

成立.

证 如果 $b>0$，则 b 的倍数当从负数到正数，由小到大列出时是

$$\cdots, -4b, -3b, -2b, -b, 0, b, 2b, 3b, 4b, \cdots$$

如果 $b<0$，则 b 的倍数当从负数到正数，由小到大列出时是

$$\cdots, 4b, 3b, 2b, b, 0, -b, -2b, -3b, -4b\cdots$$

现在有两种可能：

(1) 存在有一个整数 q，使得 $a=bq$，故 $r=0$. 本引理成立.

(2) 当 $b>0$ 时，存在有一个整数 q，使得 $qb\leqslant a<(q+1)b$. 而当 $b<0$ 时，存在有一个整数 q，使得 $qb\leqslant a<(q-1)b$. 故有 $a=bq+r$，而 $0\leqslant r<|b|$.

现在要来证明只有唯一的这样一对 q, r，使得 $a=bq+r$, $0\leqslant r<|b|$ 成立.假设还有另外一对 q_1, r_1，可使

$$a=bq_1+r_1,\quad 0\leqslant r_1<|b|$$

成立，那么将上面的二个关系式相减，得

$$0=b(q-q_1)+(r-r_1),$$

也就是 $-b(q-q_1)=r-r_1$. 所以由定义 1 有 $b|(r-r_1)$. 再根据引理 1 得 $|b|\,|\,|r-r_1|$. 因为 $0\leqslant r<|b|$, $0\leqslant r_1<|b|$，所以有

$$|r-r_1|=\begin{cases}r-r_1\leqslant r<|b|, & 当\ r\geqslant r_1\ 时,\\ r_1-r\leqslant r_1<|b|, & 当\ r<r_1\ 时.\end{cases}$$

由 $|r-r_1|<|b|$, $|b|\,|\,|r-r_1|$ 和引理 3 得到 $r-r_1=0$，也就是 $r=r_1$. 由 $b\neq 0$ 和 $b(q-q_1)=r_1-r=0$ 得到 $q-q_1=0$，也就是 $q=q_1$.

§2. 素数和复合数

1 这个数只有一个正因数，就是它本身. 任何大于 1 的正整数 a 都最少有二个正因数，就是 1 和 a.

2 只能被 1 和 2 整除，不能被其他正整数整除，同样 3 只能被 1 和 3 整除，不能被其他正整数整除．我们说 2 是素数，3 也是素数．

4 除了能被 1 和 4 整除，还能被 2 整除．6 除了能被 1 和 6 整除，还能被 2 和 3 整除．我们说 4 是复合数，6 也是复合数．

定义 2 一个大于 1 的正整数，只能被 1 和它本身整除，不能被其他正整数整除，这样的正整数叫做素数（有的书上叫做质数）．

例如 2，3，5，7，11，13，17，19 都是素数．

以后我们将常用 p 或 p_1，p_2，p_3，$\cdots$ 表示素数．

定义 3 一个正整数除了能被 1 和本身整除以外，还能被另外的正整数整除，这样的正整数叫做复合数．

例如 4，6，8，9，10，12，14，15，16，18，20 都是复合数．

由素数与复合数的定义可知，全体正整数可分为三类：

（1） 1 这个数，

（2） 全体素数，

（3） 全体复合数．

当然有无限多的复合数，比如大于 2 的偶数

$$4,6,8,10,12,\cdots$$

都是复合数．

定义 4 如果一个正整数 a 有一个因数 b，而 b 又是素数，则 b 就叫做 a 的素因数．

例如 $12=3\times4$，所以 3 和 4 都是 12 的因数，由于 3 是素数而 4 不是素数，所以 3 是 12 的素因数而 4 不是 12 的素因数．

引理 5 如果 a 是一个大于 1 的整数，则 a 的大于 1 的最小因数一定是素数．

证 如果 a 是一个素数，则 a 的大于 1 的因数只有一个，

就是 a，所以 a 的大于 1 的最小因数就是素数 a.

如果 a 是复合数，则 a 除 1 和 a 外一定有其他的正因数. 假设 b 是这些正因数中的最小的，我们将证明 b 不是复合数而是素数. 先假定 b 不是素数而是复合数，则由于 b 是复合数，所以 b 一定有大于 1 而不等于 b 的因数 c. 由 $c|b$，$b|a$ 和引理 2 有 $c|a$，即 c 是 a 的因数，又有 $1<c<b$，这与假设 b 是 a 的大于 1 的最小因数矛盾. 所以 b 不是复合数而是素数. 因此 a 的大于 1 的最小的因数 b 是素数.

这个引理说明了：任何大于 1 的整数都至少有一个素因数.

观察一个正整数 a 是不是素数，是否得用小于 a 大于 1 的整数一一来试除呢？不用.

引理 6 如果 a 是一个大于 1 的整数，而所有 $\leqslant\sqrt{a}$ 的素数都除不尽 a，则 a 是素数.

证 首先证明，如果 a 被 >1 而 $\leqslant\sqrt{a}$ 的整数都除不尽，则 a 是素数. 假设 a 是复合数而 $a=bc$，其中 b 和 c 都是大于 1 的整数. 由于 a 被 >1 而 $\leqslant\sqrt{a}$ 的整数都除不尽，所以由 $b>\sqrt{a}$，$c>\sqrt{a}$，而得 $bc>\sqrt{a}\cdot\sqrt{a}=a$，这与 $bc=a$ 是矛盾的，所以如果 a 被 >1 而 $\leqslant\sqrt{a}$ 的整数都除不尽，则 a 就是素数.

由上可知如果 a 是复合数，则 a 一定有 >1 而 $\leqslant\sqrt{a}$ 的因数. 而由引理 5 知 a 的大于 1 的最小因数一定是素数，故本引理得证.

假设 $n\geqslant 2$ 是一个整数，定义

$$a_1a_2\cdots a_n=\begin{cases}a_1a_2, & \text{当 } n=2 \text{ 时；}\\ a_1a_2a_3, & \text{当 } n=3 \text{ 时；}\\ a_1a_2a_3a_4, & \text{当 } n=4 \text{ 时；}\\ a_1a_2a_3a_4\cdots a_n, & \text{当 } n\geqslant 5 \text{ 时.}\end{cases}$$

引理 7 有无限多个素数.

证 假设素数的个数是有限多个,共有 n 个,就是 $p_1, p_2, p_3, \cdots, p_n$. 其中 $p_1 = 2, p_2 = 3, p_3 = 5, \cdots$. 令 $a = p_1 \cdots p_n + 1$, 如果 a 是素数, 则因 a 不等于 $p_1, p_2, \cdots, p_n$ 中的任何一个, 故素数的个数最少有 $n + 1$ 个而与假设素数的个数共有 n 个矛盾. 如果 a 不是素数, 则由引理 5 知道 a 的大于 1 的最小因数 b 是素数. 由于 $p_1 \cdots p_n$ 被 $p_1, p_2, \cdots, p_n$ 中的任何一个素数都除尽,但 1 被 $p_1, p_2, \cdots, p_n$ 中的任何一个素数都除不尽,所以 a 被 $p_1, p_2, \cdots, p_n$ 中的任何一个素数都除不尽. 因此 b 不等于 $p_1, \cdots, p_n$ 中的任何一个素数, 故在 $p_1, \cdots, p_n$ 以外还有素数.

§3. 素数分布的简单概况

素数的分布情况是数论中最有趣味的一个分支, 其中的推测和定理,很多都是先由经验得到的.现有的最完善的素数表是查基尔(Don Zagier)作的,他把不大于 50,000,000 的素数都列出了.(见 The Mathematical Intelligencer, 1977 年 8 月号.)

根据这个素数表可以查出素数的分布有下列情况:

在 1 到 100 中间有 25 个素数,

在 1 到 1000 中间有 168 个素数,

在 1000 到 2000 中间有 135 个素数,

在 2000 到 3000 中间有 127 个素数,

在 3000 到 4000 中间有 120 个素数,

在 4000 到 5000 中间有 119 个素数,

在 5000 到 10000 中间有 560 个素数.

所以这些数字提示我们素数的分布, 越往上越稀. 我们将 5000 以内的素数表附在本章之末. 到目前为止所知道的最大素数是 $2^{19937} - 1$. 在证明 $2^{19937} - 1$ 是一个素数时需借助于

电子计算机并用特殊方法. 我们有

$$2^{19937}-1>10^{6001}.$$

关于素数的分布有许多问题,有的已经解决了,有的直到现在还没有解决.

首先的问题是关于素数的个数问题.

在数论里经常用 $\pi(x)$ 表示不大于 x 的素数的个数. 所以 $\pi(3)=2$, $\pi(100)=25$, $\pi(1000)=168$.

现在就几个不很大的 x 把相应的 $\pi(x)$、$\frac{x}{\log x}$ 和它们的比值列表如下

x	$\pi(x)$	$\frac{x}{\log x}$	$\frac{\pi(x)}{\frac{x}{\log x}}$	$\frac{\pi(x)}{x}$
1000	168	144.764…	1.1605…	0.1680
2000	303	263.126…	1.1515…	0.1515
5000	669	587.047…	1.1396…	0.1338
10000	1229	1085.73…	1.1319…	0.1229
50000	5133	4621.166…	1.1107…	0.10266
100000	9592	8685.889…	1.1043…	0.09592

这个表提示我们三点

1) 有无限多个素数,

2) 当 x 越大时, $\pi(x)$ 与 $\frac{x}{\log x}$ 的比值越接近 1,

3) 当 x 越大时, $\pi(x)$ 与 x 的比值越接近 0.

阿达马 (Hadamard)和德·拉·瓦莱·普森(De la Vall'ee Poussin) 各自独立地在 1896 年证明了素数定理,即

$$\lim_{x\to\infty}\frac{\pi(x)}{\frac{x}{\log x}}=1.$$

由于在素数定理的证明中采用了较多的数学理论，因此

在这个地方把它详细地介绍出来，还是不适时的.

人们发现了许多相邻二个素数的差是 2，例如下列成对的素数

3，5；　5，7；　11，13；　17，19；　29，31；

41，43；　59，61；　71，73；　101，103；　…

可以叫作双生素数. 人们要问是否有无限多对双生素数呢？这个问题的解答非常困难. 华罗庚、王元、潘承洞、丁夏畦、尹文霖和陈景润都曾经在这方面进行过不少工作. 这个问题现在最好的结果是：存在有无限多个素数 p，使得 $p+2$ 为不超过二个素数之积. 现在我们所知道的最大素数对是

$$76\times 3^{169}-1,\quad 76\times 3^{169}+1.$$

这个结果是威廉斯（Willams）和察恩克（Zarnke）得到的.（见 Tom M. Apostol Intro. to Analytic Number Theory，1976.）

某些数字资料建议：相邻二个素数的差是 2 的素数对可能有无限多对.

我们有

$6=3+3$，　$8=3+5$，　$10=5+5$，

$12=5+7$，　$14=7+7$，　$16=3+13$，

$18=5+13$，　$20=7+13$，　$22=3+19$，

$24=5+19$，　$26=3+23$，　$28=5+23$，…

由此提示可能有：凡大于 4 的偶数都是二个奇素数之和，这就是著名的哥德巴赫（Goldbach）猜想.

这个哥德巴赫猜想直到现在还没有肯定的或否定的答案，我们认为哥德巴赫猜想是肯定的可能性很大. 这个问题现在最好的结果是：每一充分大的偶数都是一个素数及一个不超过二个素数的乘积之和. 华罗庚、王元、潘承洞、丁夏畦、尹文霖和陈景润都曾经在这方面进行过不少工作.

默森尼（Mersenne）曾经研究过形状为 2^p-1 的素数，

其中 p 代表素数. 他在 1644 年证明了,当 p 是下列的 9 个素数之一,即

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 127$$

时,则 $2^p - 1$ 是素数. 由于默森尼在这个问题上的贡献,人们把形状为 $2^p - 1$ 的正整数叫作默森尼数. 是否存在有无限多个默森尼数是素数,这也是数论中的一个难题.

到目前为止,所知道的默森尼数

$$M_p = 2^p - 1$$

是素数的,已有 24 个. 即当

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937$$ 时,则 $2^p - 1$ 都是素数.

当 $n \geqslant 0$ 是一个整数时,人们把形状为 $2^{2^n} + 1$ 的正整数叫作费尔马 (Fermat) 数,并记为 $F_n = 2^{2^n} + 1$. 最前面的五个费尔马数是

$$F_0 = 2^{2^0} + 1 = 2 + 1 = 3,$$
$$F_1 = 2^{2^1} + 1 = 2^2 + 1 = 5,$$
$$F_2 = 2^{2^2} + 1 = 2^4 + 1 = 17,$$
$$F_3 = 2^{2^3} + 1 = 2^8 + 1 = 257,$$
$$F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65537.$$

由于 3, 5, 17, 257, 65537 都是素数,所以费尔马猜测当 $n \geqslant 0$ 时所有 F_n 都是素数, 但是费尔马的猜测并不正确, 因为 $F_5 = 2^{2^5} + 1$ 不是素数(见习题 (29)).

§4. 最大公因数和最小公倍数

10 有因数 1, 2, 5, 10, 而 15 有因数 1, 3, 5, 15, 所以 1 是 10 和 15 的公因数, 5 也是 10 和 15 的公因数.

几个正整数的公因数有时候不止一个.

例如 12 和 30 的公因数有 1，2，3，6 四个．在这四个数里最大的一个是 6，6 就叫做 12 和 30 的最大公因数．

定义 5 如果 $n \geqslant 2$ 是整数，而 $a_1, a_2, \cdots, a_n$ 和 d 都是正整数（当 $n=2$ 时，$a_1, a_2, \cdots, a_n$ 表示 a_1, a_2；当 $n=3$ 时，$a_1, a_2, \cdots, a_n$ 表示 a_1, a_2, a_3；而当 $n=4$ 时，$a_1, a_2, \cdots, a_n$ 表示 a_1, a_2, a_3, a_4；等等）．又设

$$d \mid a_1,\ d \mid a_2,\ \cdots,\ d \mid a_n,$$

则 d 叫做 $a_1, a_2, \cdots, a_n$ 的公因数．公因数中的最大的那一个数叫做 $a_1, a_2, \cdots, a_n$ 的最大公因数，最大公因数是其他所有公因数的倍数．如果 d 是 $a_1, a_2, \cdots, a_n$（这些数）的最大公因数，我们就写作

$$(a_1, a_2, \cdots, a_n) = d.$$

例 1 求 36 和 24 的最大公因数．

解 把这二个数分别分解素因数

$$36 = 2 \times 2 \times 3 \times 3, \quad 24 = 2 \times 2 \times 2 \times 3.$$

把这二个数的素因数比较一下，可以看出素因数 2，2，3 是这二个数所公有的，它们的乘积就是这二个数的最大公因数：

$$2 \times 2 \times 3 = 12.$$

求几个正整数的最大公因数，先把这些正整数分别分解素因数，然后取出它们所公有的素因数（相同的素因数照公有的个数取）相乘．

例 2 求 48、60 和 72 的最大公因数．

解 把这三个数分别分解素因数

$$48 = 2 \times 2 \times 2 \times 2 \times 3 = 2^4 \times 3,$$

$$60 = 2 \times 2 \times 3 \times 5 = 2^2 \times 3 \times 5,$$

$$72 = 2 \times 2 \times 2 \times 3 \times 3 = 2^3 \times 3^2.$$

把上面三个数的素因数比较一下，可以看出素因数 2，2，

3 (或 2^2, 3) 是这三个数所公有的，它们的乘积就是这三个数的最大公因数

$$2\times 2\times 3=12 \text{ 或 } 2^2\times 3=12.$$

为通俗起见，先讨论最大公因数和最小公倍数，再讨论算术基本定理. 求几个数的最大公因数，先把这些数分别分解素因数，并且写成乘方形式；然后在各个公有的素因数里，取出指数最小的乘方相乘.

例 3 求 1008, 1260, 882 和 1134 的最大公因数.

解 把这四个数分别分解素因数

$1008=2\times 2\times 2\times 2\times 3\times 3\times 7=2^4\times 3^2\times 7$,

$1260=2\times 2\times 3\times 3\times 5\times 7=2^2\times 3^2\times 5\times 7$,

$882=2\times 3^2\times 7^2$,

$1134=2\times 3^4\times 7$.

所以 $(1008, 1260, 882, 1134)=2\times 3^2\times 7=126$.

引理 8 假设 a 和 b 都是正整数，且 $a>b$,

$$a=bq+r,\quad 0<r<b,$$

其中 q 和 r 都是正整数，则 a 和 b 的最大公因数等于 b 和 r 的最大公因数，即

$$(a, b)=(b, r).$$

证 设 $(a, b)=d$. 由定义 5 有二个整数 m, n 使得 $a=dm$, $b=dn$. 由 $r=a-bq=(m-qn)d$, 所以 $d|r$, 由 $d|r$, $d|b$, 所以 $d|(b, r)$ 即 $(b, r)\geqslant d$. 假设 $(b, r)=D>d$, 则 $D|b$, $D|r$. 由 $a=bq+r$ 所以 $D|a$. 由 $D|a$, $D|b$ 所以 $D|(a, b)$ 即 $(a, b)=d\geqslant D$, 此与假设 $(b, r)=D>d$ 矛盾，所以 $(b, r)=d$. 因此 $(a, b)=d=(b, r)$.

如果有 n 个正整数 $a_1, a_2, \cdots, a_n$, 其中 $n\geqslant 2$, 而每个正整数都不是很大时，则将其中所有的 a_i 都分别分解素因数，我们可以很快地得到这 n 个正整数 $a_1, a_2, \cdots, a_n$ 的最大

公因数．但是当这 n 个正整数 $a_1, a_2, \cdots, a_n$ 中有些 a_i 是相当大时，则不容易将它们分解成素因数相乘．遇到这样困难的时候，我们可以使用辗转相除法．

辗转相除法 假设 a 和 b 都是正整数，且 $a > b$．如果我们要求 a 和 b 的最大公因数，可先以 b 除 a．由引理 4 得到

$$a = bq_1 + r_1,$$

其中 q_1 和 r_1 都是非负整数，而 $0 \leqslant r_1 < b$．如果 $r_1 = 0$，则有 $a = bq_1$，所以 a 和 b 的最大公因数就是 b．如果 $r_1 \neq 0$，这时则有 $0 < r_1 < b$．我们再以 r_1 除 b，由引理 4 得到

$$b = r_1q_2 + r_2,$$

其中 q_2 和 r_2 都是非负整数，而 $0 \leqslant r_2 < r_1$．由 $a = bq_1 + r_1$，$0 < r_1 < b$ 和引理 8 我们有

$$(a, b) = (b, r_1).$$

如果 $r_2 = 0$，则 b 和 r_1 的最大公因数就是 r_1，即 $(b, r_1) = r_1$，由 $(a, b) = (b, r_1)$ 得到 a 和 b 的最大公因数就是 r_1．如果 $r_2 \neq 0$，则有 $0 < r_2 < r_1$．我们再以 r_2 除 r_1，由引理 4 得到

$$r_1 = r_2q_3 + r_3,$$

其中 q_3 和 r_3 都是非负整数，而 $0 \leqslant r_3 < r_2$．由 $b = r_1q_2 + r_2$，$0 < r_2 < r_1$ 和引理 8，我们有

$$(b, r_1) = (r_2, r_1).$$

由 $(a, b) = (b, r_1)$ 得到 $(a, b) = (r_2, r_1)$．如果 $r_3 = 0$，则有 $(r_1, r_2) = r_2$，所以 $(a, b) = r_2$．如果 $r_3 \neq 0$，则有 $0 < r_3 < r_2$．我们再以 r_3 除 r_2，

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

这样继续辗转相除．由于 $b > r_1 > r_2 > r_3 > \cdots$ 和所有 r_i $(i = 1, 2, 3, \cdots)$ 都是非负整数，所以一定存在有一个正整

数 n，使得经过 $n+1$ 次辗转相除后有 $r_{n+1}=0$，但 $r_n \neq 0$，这时 r_n 就是 a 和 b 的最大公因数，即 $(a, b)=r_n$.

例 4　求 6731 和 2809 的最大公因数

解

$$6731 = 2809 \times 2 + 1113,$$
$$2809 = 1113 \times 2 + 583,$$
$$1113 = 583 \times 1 + 530,$$
$$583 = 530 + 53,$$
$$530 = 53 \times 10 + 0.$$

所以 $(6731, 2809) = 53$. 为了书写方便起见，上面一系列的计算可以简写如下

	6731	2809	2
	5618	2226	
2	1113	583	1
	583	530	
1	530	53	10
	530	(0)	
	0	53	

.

设 $n \geqslant 3$ 是一个正整数，$a_1, a_2, \cdots, a_n$ 都是正整数. 这里我们介绍一种求这 n 个正整数 $a_1, a_2, \cdots, a_n$ 的最大公因数的办法：我们先求 a_1 和 a_2 的最大公因数，如果 a_1 和 a_2 的最大公因数是 b_1. 然后我们再求 b_1 和 a_3 的最大公因数，如果 b_1 和 a_3 的最大公因数是 b_2，则 b_2 就是 a_1，a_2 和 a_3 的最大公因数. 当 $n \geqslant 4$ 时，我们再求 b_2 和 a_4 的最大公因数，如果 b_2 和 a_4 的最大公因数是 b_3，则 b_3 就是 a_1，a_2，a_3 和 a_4 的最大公因数. 当 $n \geqslant 5$ 时，我们再求 b_3 和 a_5 的最大公因数，$\cdots$.

例 5　求 735000，421160 和 238948 的最大公因数.

解

$$735000 = 238948 \times 3 + 18156,$$
$$238948 = 18156 \times 13 + 2920,$$
$$18156 = 2920 \times 6 + 636,$$
$$2920 = 636 \times 4 + 376,$$
$$636 = 376 \times 1 + 260,$$
$$376 = 260 \times 1 + 116,$$
$$260 = 116 \times 2 + 28,$$
$$116 = 28 \times 4 + 4,$$
$$28 = 7 \times 4 + 0.$$

所以 735000 和 238948 的最大公因数是 4，由于 $4 \mid 421160$，故得

$$(735000, 238948, 421160) = 4.$$

上面一系列的计算可以简写如下

	735000	238948	3
	716844	236028	
13	18156	2920	6
	17520	2544	
4	636	376	1
	376	260	
1	260	116	2
	232	112	
4	28	4	7
	28		
	0	4	.

例 6 求 $(27090, 21672, 11352, 8127)$.

解 由于

	27090	21672	1
	21672	21672	
4	5418	0	

，

得到 $(27090, 21672) = 5418$. 由于

	11352	5418	2
	10836	5160	
10	516	258	2
	516		
	0	258	

，

得到 $(11352, 5418) = 258$. 由于

	8127	258	31
	7998	258	
2	129	0	

，

得到 $(8127, 258) = 129$, 故得

$$(27090, 21672, 11352, 8127) = 129.$$

定义 6 如果 $n \geqslant 2$ 是整数，而 $a_1, a_2, \cdots, a_n$ 都是正整数，当这些正整数的最大公因数是 1，也就是 $(a_1, a_2, \cdots, a_n) = 1$ 时，我们就说，$a_1, a_2, \cdots, a_n$ 是互素的.

在互素的正整数中，不一定有素数. 例如 $(25, 36) = 1$，但 25 和 36 都不是素数而都是复合数.

在个数不少于 3 个的互素的正整数中，不一定是每二个正整数都是互素的. 例如 $(6, 10, 15) = 1$，但 $(6, 10) = 2$，$(6, 15) = 3$，$(10, 15) = 5$.

一个正整数能被几个正整数整除时，则这个正整数就叫做这几个正整数的公倍数. 例如 24 能被 6 整除，24 还能被

8 整除，所以 24 是 6 和 8 的公倍数. 48 是 12 和 8 的公倍数.

定义 7 如果 $n \geq 2$ 是整数，而 $a_1, a_2, \cdots, a_n$ 和 m 都是正整数，又

$$a_1 | m, \ a_2 | m, \ \cdots, \ a_n | m,$$

则 m 叫做 $a_1, a_2, \cdots, a_n$ 的公倍数.

如果 $n \geq 2$ 是整数，而 $a_1, a_2, \cdots, a_n$ 和 k 都是正整数，由于 $a_1 | k a_1 a_2 \cdots a_n$, $a_2 | k a_1 a_2 \cdots a_n$, $\cdots$, $a_n | k a_1 a_2 \cdots a_n$, 所以 $k a_1 a_2 \cdots a_n$ 是 $a_1, a_2, \cdots, a_n$ 的公倍数. 由于 k 可取 1, 2, 3, $\cdots$，所以有无限多个不同的正整数，它们都是 $a_1, a_2, \cdots, a_n$ 的公倍数. 在 $a_1, a_2, \cdots, a_n$ 所有的公倍数中，其中最小的那一个公倍数就叫做 $a_1, a_2, \cdots, a_n$ 的最小公倍数. 如果 m 是 $a_1, a_2, \cdots, a_n$ 的最小公倍数，我们就写作

$$\{a_1, a_2, \cdots, a_n\} = m.$$

由于 12 能被 4 整除，12 能被 6 整除，所以 12 是 4 和 6 的公倍数. 又由于不存在小于 12 的正整数，同时能够被 4 和 6 都整除，所以 12 是 4 和 6 的最小公倍数，即 $\{4, 6\} = 12$.

如果想求 n 个正整数 $a_1, a_2, \cdots, a_n$ 的最小公倍数，可先把它们都分解成素因数. 然后再观察它们都有些什么不同的素因数. 设 $p_1, p_2, \cdots, p_s$ 是全体出现在这 n 个正整数 $a_1, a_2, \cdots, a_n$ 中的不同的素因数. 当 $1 \leqslant i \leqslant s$ 时我们定义 β_i 是一个正整数，它使得

$$p_i^{\beta_i+1} \nmid a_1, \ p_i^{\beta_i+1} \nmid a_2, \ \cdots, \ p_i^{\beta_i+1} \nmid a_n,$$

但是在这 n 个正整数 $a_1, a_2, \cdots, a_n$ 中至少存在有一个 a_j 而具有 $p_i^{\beta_i} | a_j$, 那么

$$p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$$

就是这 n 个数 $a_1, a_2, \cdots, a_n$ 的最小公倍数.

例 7 求 108，28 和 42 的最小公倍数.

解 由于

$$108 = 2^2 \times 3^3,\ 28 = 2^2 \times 7,\ 42 = 2 \times 3 \times 7,$$

故得

$$\{108, 28, 42\} = 2^2 \times 3^3 \times 7 = 756.$$

例 8 求 198，240 和 360 的最小公倍数.

解 由于

$$198 = 2 \times 3^2 \times 11,\ 240 = 2^4 \times 3 \times 5,\ 360 = 2^3 \times 3^2 \times 5,$$

故得

$$\{198, 240, 360\} = 2^4 \times 3^2 \times 5 \times 11 = 7920.$$

注意：(1) 几个正整数里，如果最大的一个正整数是其他各个正整数的倍数，则最大的那一个正整数，就是这几个正整数的最小公倍数，例如 15，30 和 60 的最小公倍数是 60.

(2) 几个正整数里，如果任意二个数都是互素的，则这几个正整数的最小公倍数就是它们的相乘积. 例如 15，32 和 49 的最小公倍数就是

$$15 \times 32 \times 49 = 23520.$$

引理 9 假设 a 和 b 都是正整数，而 a 和 b 的最小公倍数是 m，即 $\{a, b\} = m$. 如果 m' 是 a 和 b 的公倍数，则有

$$m \mid m'.$$

证 因为 m' 是 a 和 b 的公倍数，而 m 是 a 和 b 的最小公倍数，所以有 $1 \leqslant m \leqslant m'$. 由引理 4 有

$$m' = mq + r,$$

其中 q 和 r 都是非负整数，而 $0 \leqslant r < m$. 由于 m 是 a 和 b 的最小公倍数，而 m' 是 a 和 b 的公倍数，所以有

$$a \mid m, \quad b \mid m, \quad a \mid m', \quad b \mid m'.$$

设 $m = aa'$，$m' = aa''$，$m = bb'$，$m' = bb''$，其中 a'，a''，b'，

b'' 都是整数．如果 $1 \leqslant r < m$，则由于 $m' - mq = r$ 得到

$$a(a'' - a'q) = r, \quad b(b'' - b'q) = r.$$

由于 $a'' - a'q$ 和 $b'' - b'q$ 都是整数，所以有 $a|r$，$b|r$，即 r 是 a 和 b 的公倍数，但由于 $1 \leqslant r < m$ 和 m 是 a 和 b 的最小公倍数发生矛盾，所以有 $r = 0$，即 $m' = mq$.

引理 10 假设 a 和 b 都是正整数，a 和 b 的最大公因数是 d 而 a 和 b 的最小公倍数是 m，即 $(a, b) = d$ 而 $\{a, b\} = m$，则我们有

$$ab = dm.$$

证 因 ab 是 a 和 b 的公倍数而 m 是 a 和 b 的最小公倍数，所以由引理 9 有

$$ab = mq,$$

其中 q 是正整数．由 $ab = mq$ 得到 $\frac{a}{q} = \frac{m}{b}$，$\frac{b}{q} = \frac{m}{a}$．由于 $\frac{m}{b}$ 和 $\frac{m}{a}$ 都是正整数，所以 $\frac{a}{q}$ 和 $\frac{b}{q}$ 也都是正整数，即 $q|a$，$q|b$，因而 q 是 a 和 b 的公因数．

设 g 是 a 和 b 的另一公因数，令 $m' = \frac{ab}{g}$．由于 $\frac{a}{g}$，$\frac{b}{g}$ 都是正整数和 $m' = a \times \left(\frac{b}{g}\right) = \left(\frac{a}{g}\right) \times b$，所以 m' 是 a 和 b 的公倍数．由引理 9 有 $m|m'$，即 $\frac{m'}{m}$ 是一个正整数．又由

$$\frac{m'}{m} = \frac{ab}{(g)\left(\frac{ab}{q}\right)} = \frac{q}{g}$$

得到 g 是 q 的因数．由于 q 是 a 和 b 的公因数，而 a 和 b 的任一公因数都能除尽 q，所以 q 就是 a 和 b 的最大公因数．

例 9 求 24871 和 3468 的最小公倍数．

解 由于

	24871	3468	7
	24276	2975	
5	595	493	1
	493	408	
4	102	85	1
	85	85	
5	17	0	

，

所以 $(24871, 3468) = 17$. 由引理 10 我们有

$$\{24871, 3468\} = \frac{24871 \times 3468}{17} = 5073684.$$

设 $n \geqslant 3$ 是一个正整数，而 $a_1, a_2, \cdots, a_n$ 都是正整数. 这里我们再介绍一种求这 n 个正整数 $a_1, a_2, \cdots, a_n$ 的最小公倍数的办法：我们先求 a_1 和 a_2 的最小公倍数，如果 a_1 和 a_2 的最小公倍数是 b_1，然后我们再求 b_1 和 a_3 的最小公倍数，如果 b_1 和 a_3 的最小公倍数是 b_2，则 b_2 就是 a_1，a_2 和 a_3 的最小公倍数. 当 $n \geqslant 4$ 时，我们再求 b_2 和 a_4 的最小公倍数，如果 b_2 和 a_4 的最小公倍数是 b_3，则 b_3 就是 a_1, a_2, a_3 和 a_4 的最小公倍数. 当 $n \geqslant 5$ 时，我们再求 b_3 和 a_5 的最小公倍数，$\cdots$.

例 10 求 513，135 和 3114 的最小公倍数.

解 由于

	513	135	3
	405	108	
1	108	27	4
	108		
	0	27	

，

所以 $(513, 135) = 27$，由引理 10 我们有

$$\{513, 135\} = \frac{513 \times 135}{27} = 2565.$$

由于

1	2565	3114	
	2196	2565	
1	369	549	4
	360	369	
20	9	180	2
		180	
	9	0	

，

所以 $(2565, 3114) = 9$，由引理 10 我们有

$$\{2565, 3114\} = \frac{2565 \times 3114}{9} = 887490,$$

所以

$$\{513, 135, 3114\} = 887490.$$

例 11 求 8127，11352，21672 和 27090 的最小公倍数．

解 由于

1	8127	11352	
	6450	8127	
1	1677	3225	2
	1548	1677	
12	129	1548	1
		1548	
	129	0	

，

所以 $(8127, 11352) = 129$，由引理 10 我们有

$$\{8127, 11352\} = \frac{8127 \times 11352}{129} = 715176.$$

由于

$$
\begin{array}{r|r|r|l}
 & 715176 & 21672 & 33 \\
 & 715176 & & \\
\hline
 & 0 & 21672 &
\end{array},
$$

所以 (715176, 21672) = 21672，而由引理 10 我们有

$$
\{715176, 21672\} = \frac{715176 \times 21672}{21672} = 715176.
$$

由于

$$
\begin{array}{r|r|r|l}
 & 715176 & 27090 & 26 \\
 & 704340 & 21672 & \\
\hline
2 & 10836 & 5418 & 2 \\
 & 10836 & & \\
\hline
 & 0 & 5418 &
\end{array},
$$

所以 (715176, 27090) = 5418，而由引理 10 我们有

$$
\{715176, 27090\} = \frac{715176 \times 27090}{5418} = 3575880,
$$

故得

$$
\{8127, 11352, 21672, 27090\} = 3575880.
$$

§5. 最大公因数和最小公倍数的应用

例 12 一块钢板，长 1 丈 3 尺 5 寸，宽 1 丈零 5 寸．现在把它截成同样大小的正方形，正方形要最大的，并且不许剩下钢板．求正方形的边长．

解 因为正方形要最大的，所以就要求正方形最大的边长是多少．要求正方形最大的边长，就要求 135 寸和 105 寸的最大公因数．由于

$$
135 = 3^3 \times 5, \quad 105 = 3 \times 5 \times 7,
$$

所以 $(135, 105) = 15$.

答：正方形的边长是1尺5寸.

例 13 有钢丝三根，一长13尺5寸，一长24尺3寸，一长55尺8寸. 现在要把它们截成相等的小段，每根都不许剩下，截成的小段要最长，求每小段长几寸？一共可以截成多少段？

解 由于

$$135 = 3^3 \times 5, \quad 243 = 3^5, \quad 558 = 2 \times 3^2 \times 31,$$

所以 $(135, 243, 558) = 9$. 又有

$$\frac{135}{9} + \frac{243}{9} + \frac{558}{9} = 15 + 27 + 62 = 104.$$

答：截成的小段每段长9寸，一共可以截成104段.

例 14 甲乙二个齿轮，互相衔接，甲轮有437齿，乙轮有323齿. 甲的某一齿和乙的某一齿相接触后到再互相接触，最少各要转几周？

解 要求最少各转几周，就要先求甲乙二轮都转过多少齿. 要求甲乙二轮都转过多少齿，就要先求甲轮的齿数(437)和乙轮齿数(323)的最小公倍数. 由于

	437	323	1
	323	228	
2	114	95	1
	95	95	
5	19	0	

,

所以 $(437, 323) = 19$，由引理10我们有

$$\{437, 323\} = \frac{437 \times 323}{19} = 7429,$$

所以甲轮转的周数：$7429 \div 437 = 17$ 周，

乙轮转的周数：$7429 \div 323 = 23$ 周.

例 15 有三个工人从砖垛往砌墙的脚手架上运砖，来回一次甲要 15.6 分钟，乙要 16.8 分钟，丙要 18.2 分钟，现在三人同时从砖垛处出发，最少要几分钟三人又同时回到砖垛处？

解 要求出最少要几分钟三人又同时回到砖垛处，就要求 15.6，16.8 和 18.2 的最小公倍数．由于

$$\begin{array}{r|r|r|l} 1 & 15.6 & 16.8 & \\ & 15.6 & 15.6 & \\ \hline & 0 & 1.2 & 13, \end{array}$$

所以 $(15.6, 16.8) = 1.2$，由引理 10 我们有

$$\{15.6, 16.8\} = \frac{15.6 \times 16.8}{1.2} = 218.4,$$

由于 $\frac{218.4}{18.2} = 12$，所以 $\{15.6, 16.8, 18.2\} = 218.4$.

所以最少需要 218.4 分即 3 时 38.4 分后三人才能够同时回到砖垛处.

§6. 算术基本定理

引理 11 每一个大于 1 的整数 a 都可以分解成素因数的连乘积，就是

$$a = p_1 \cdots p_n, \quad n \geqslant 1$$

这里 $p_1, \cdots, p_n$ 都是素数，其中可能有相同的，例如 $12 = 2 \times 2 \times 3$，$18 = 2 \times 3 \times 3$.

证 当 a 是一个素数 p，就是 $a = p$，那么就不用再分解了．如果 a 是一个复合数，则由引理 5 可知，它的大于 1 的最小因数是素数．设此素数是 p_1，由于 a 是复合数而 p_1 是 a 的因数，所以有 $a = p_1a_1$，其中 a_1 是一个大于 1 的整数．如果

a_1 是素数 p_2，就得到 $a = p_1p_2$. 如果 a_1 不是素数而是复合数，则由引理 5 可知，它的大于 1 的最小因数是素数. 设此素数是 p_2 并且有 $a_1 = p_2a_2$，如果 a_2 是素数，就不用再分解了. 如果 a_2 是复合数，则同理可得 $a_2 = p_3a_3$. 这样做下去，因为 $a_1 > a_2 > \cdots$，故最后必得

$$a = p_1\cdots p_n, \quad n \geqslant 1.$$

一般地讲来，如果 $a\nmid b$，则不一定是 $(a, b) = 1$，例如 $4\nmid 6$，$6\nmid 9$，但是 $(4, 6) = 2$，$(6, 9) = 3$.

引理 12 如果 p 是一个素数，则由 $p\nmid a$ 可得 $(p, a) = 1$，而当 $(p, a) = 1$ 时可得 $p\nmid a$.

证 由于 p 是一个素数，所以 p 只有二个正因数，即 1 和 p. 如果 $p\nmid a$，则只有 $(p, a) = 1$ 了. 反之，如果 $(p, a) = 1$，则 p 不是 p 和 a 的公因数，所以 $p\nmid a$.

引理 13 如果 a, b, c 都是正整数，则由 $(a, b) = 1$，$a|bc$ 可得 $a|c$. 这就是说：当 a 和 b 互素，但是 a 能除尽 bc 时，那么一定是 a 能除尽 c.

证 因为 $b|bc$ 和 $a|bc$，所以 bc 是 a 和 b 的公倍数. 由于 $(a, b) = 1$ 和引理 10，所以 a 和 b 的最小公倍数是 ab. 由引理 9 有 $ab|bc$，即 $\frac{bc}{ab} = \frac{c}{a}$ 是一个整数，所以 $a|c$.

引理 14 如果 $n \geqslant 2$ 是一个整数，而 $a_1, a_2, \cdots, a_n$ 和 a 都是正整数. 当 $a|a_1a_2\cdots a_n$ 和

$$(a, a_1) = (a, a_2) = \cdots = (a, a_{n-1}) = 1$$

时，那么一定有 $a|a_n$.

证 由 $(a, a_1) = 1$，$a|a_1a_2\cdots a_n$ 和引理 13 我们有 $a|a_2\cdots a_n$. 故当 $n = 2$ 时本引理成立. 如果 $n \geqslant 3$，则由 $(a, a_2) = 1$，$a|a_2a_3\cdots a_n$ 和引理 13 我们有 $a|a_3\cdots a_n$，故当 $n = 3$ 时本引理成立. 如果 $n \geqslant 4$，用同样办法做下去，可得

$a|a_{n-1}a_n$. 由 $(a, a_{n-1})=1$、$a|a_{n-1}a_n$ 和引理 13 得到 $a|a_n$.

引理 15 如果 a, b, c 都是正整数，而 $(a, b)=1$, $c|a$, 则有

$$(b, c)=1.$$

证 如果 $(b, c)=d$, 而 $d>1$, 则有 $d|b$, $d|c$. 由 $d|c$ 和 $c|a$ 有 $d|a$. 由于 $d|a$, $d|b$, 所以 d 是 a 和 b 的公因数，但是 $d>1$ 而 a 和 b 的最大公因数是 1, 这和定义 5 发生矛盾，所以 $(b, c)=1$.

引理 16 如果 a 和 b 都是正整数，而 $(a, b)=1$, 则有

$$(a, bc)=(a, c).$$

证 设 $(a, c)=d_1$, 而 $(a, bc)=d_2$, 则有 $d_1|a$, $d_1|c$, $d_2|a$, $d_2|bc$. 由 $d_1|c$ 得到 $d_1|bc$. 由 $d_1|a$, $d_1|bc$ 得到 d_1 也是 a 和 bc 的公因数，但是 d_2 是 a 和 bc 的最大公因数，故由定义 5 有

$$d_1 \leqslant d_2. \tag{1}$$

另外由 $d_2|a$, $(a, b)=1$ 和引理 15 得到 $(d_2, b)=1$. 由 $(d_2, b)=1$, $d_2|bc$ 和引理 13 得到 $d_2|c$. 由 $d_2|a$, $d_2|c$ 得到 d_2 也是 a 和 c 的公因数，但是 d_1 是 a 和 c 的最大公因数，故由定义 5 有

$$d_2 \leqslant d_1. \tag{2}$$

由 (1) 式和 (2) 式得到 $d_1=d_2$, 故有 $(a, bc)=(a, c)$.

引理 17 如果 $n \geqslant 2$ 是一个整数，而 $b_1, b_2, \cdots, b_n$ 和 a 都是正整数，当 $(a, b_1)=(a, b_2)=\cdots=(a, b_n)=1$ 时则有

$$(a, b_1b_2\cdots b_n)=1.$$

证 由 $(a, b_1)=1$ 和引理 16 得到

$$(a, b_1b_2\cdots b_n)=(a, b_2\cdots b_n),$$

再由 $(a, b_2)=1$ 和引理 16 得到 $(a, b_2\cdots b_n)=(a, b_3\cdots b_n)$,

所以

$$
\begin{aligned}
(a, b_1b_2\cdots b_n) &= (a, b_2b_3\cdots b_n) \\
&= (a, b_3\cdots b_n) \\
&\cdots\cdots\cdots\cdots \\
&= (a, b_n) = 1.
\end{aligned}
$$

引理 18 如果 $n \geqslant 2$ 是一个整数，$a_1, a_2, \cdots, a_n$ 都是正整数，而 p 是一个素数，当 $p|a_1a_2\cdots a_n$ 时，则至少存在有一个 a_r 能被 p 除尽，也就是 $p|a_r$.

证 假设 p 除不尽任何一个 $a_i(i = 1, 2, \cdots, n)$. 从 p 是一个素数及引理 12，我们得到

$$(p, a_1) = (p, a_2) = \cdots = (p, a_n) = 1,$$

故由引理 17 得到 $(p, a_1a_2\cdots a_n) = 1$. 由 $(p, a_1a_2\cdots a_n) = 1$ 和引理 12 我们有 $p \nmid a_1a_2\cdots a_n$. 此与题设 $p|a_1a_2\cdots a_n$ 矛盾，所以假设 p 除不尽任何 $a_i(i = 1, 2, \cdots, n)$ 是不对的，故必有一个 a_r，使得 $p|a_r$.

引理 19 如果 $n \geqslant 2$ 是一个整数，而 $p_1, p_2, \cdots, p_n$ 和 p 都是素数，当 $p|p_1p_2\cdots p_n$ 时，则最少必有一个 p_r，而 r 是 $1, 2, \cdots, n$ 中的某一个数，它使得 $p = p_r$.

证 由 $p|p_1p_2\cdots p_n$ 和引理 18 知道，最少必有一个素数 p_r，使得 $p|p_r$. 由于 p_r 是一个素数，所以它只有二个正因数，即 1 和 p_r. 由 $p \neq 1$ 和 $p|p_r$，所以有 $p = p_r$.

如果把一个正整数写成正因数的连乘积，常常能写出多种形式，例如 $60 = 2 \times 30 = 3 \times 20 = 4 \times 15 = 6 \times 10 = 12 \times 5 = 2 \times 3 \times 10 = 2 \times 2 \times 15 = 3 \times 4 \times 5 = 2 \times 6 \times 5 = 2 \times 3 \times 2 \times 5$.

定理 1 （算术基本定理） 如果不计素因数的次序，则只有一种方法可以把一个正整数 $a > 1$ 分解成素因数的连乘积。

证 如果 a 是一个素数 p，就是 $a=p$，本定理成立．如果 a 是一个复合数，则由引理 11 可知，a 是可以分解成素因数的连乘积的．设

$$a=p_1p_2\cdots p_n,\quad n\geqslant 2$$

其中 $p_1, p_2, \cdots, p_n$ 都是素数．假设 a 能被分解成另一种形式的素因数连乘积，就是

$$a=q_1q_2\cdots q_m,\quad m\geqslant 2$$

其中 $q_1, q_2, \cdots, q_m$ 都是素数，那么我们得到

$$p_1p_2\cdots p_n=q_1q_2\cdots q_m. \tag{3}$$

由于 $p_1|p_1p_2\cdots p_n$ 和 (3) 式，所以有 $p_1|q_1q_2\cdots q_m$．由于 q_1, $q_2, \cdots, q_m$ 都是素数，所以由引理 19 得到：p_1 必等于一个 q_r，而 r 是 $1, 2, \cdots, m$ 中的一个．设 $p_1=q_1$，则由 (3) 式得到

$$p_2\cdots p_n=q_2\cdots q_m. \tag{4}$$

当 $n=2$ 时，由于 $p_2\cdots p_n=p_2$，所以有 $m=2$，$q_2=p_2$．现设 $n\geqslant 3$，由于 $p_2|p_2\cdots p_n$ 和 (4) 式，所以有 $p_2|q_2\cdots q_m$．由于 $q_2, \cdots, q_m$ 都是素数，所以由引理 19 得到：p_2 必等于一个 q_s，而 s 是 $2, \cdots, m$ 中的一个．设 $p_2=q_2$，则由 (4) 式得到

$$p_3\cdots p_n=q_3\cdots q_m.$$

当 $n=3$ 时，由于 $p_3\cdots p_n=p_3$，所以有 $m=3$，$q_3=p_3$．如果 $n\geqslant 4$，用同样的方法做下去，因为那些 p 和那些 q 恒是一一对应并且相等，故消来消去，最后必得 $p_n=q_m$，这就是说 $m=n$．所以 a 被分解成素因数的连乘积，在不计素因数的次序时，只能有一种方法．

由此定理可知，如果把相同的素因数合并为它的幂数，则任一个整数 $a>1$，只能分解成一种形式：

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n},\quad n\geqslant 1$$

在这里 $p_1, p_2, \cdots, p_n$ 是各不相同的素数，$\alpha_1, \alpha_2, \cdots, \alpha_n$ 都是正整数．我们把

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$

叫作 a 的标准分解式.

例 16 求 117 的标准分解式.

解

$$\begin{array}{r|l} 3 & 117 \\ \hline 3 & 39 \\ \hline & 13 \end{array}$$

所以 $117 = 3^2 \times 13$.

例 17 求 9828 的标准分解式。

解

$$\begin{array}{r|l} 2^2 & 9828 \\ \hline 3 & 2457 \\ \hline 3^2 & 819 \\ \hline 7 & 91 \\ \hline & 13 \end{array}$$

所以 $9828 = 2^2 \times 3^3 \times 7 \times 13$.

例 18 求 10725 的标准分解式。

解

$$\begin{array}{r|l} 3 & 10725 \\ \hline 5^2 & 3575 \\ \hline 11 & 143 \\ \hline & 13 \end{array}$$

所以 $10725 = 3 \times 5^2 \times 11 \times 13$.

5000以内的素数表

p	p	p	p	p	p	p	p
2	139	331	541	751	983	1217	1459
3	149	337	547	757	991	1223	1471
5	151	347	557	761	997	1229	1481
7	157	349	563	769	1009	1231	1483
11	163	353	569	773	1013	1237	1487
13	167	359	571	787	1019	1249	1489
17	173	367	577	797	1021	1259	1493
19	179	373	587	809	1031	1277	1499
23	181	379	593	811	1033	1279	1511
29	191	383	599	821	1039	1283	1523
31	193	389	601	823	1049	1289	1531
37	197	397	607	827	1051	1291	1543
41	199	401	613	829	1061	1297	1549
43	211	409	617	839	1063	1301	1553
47	223	419	619	853	1069	1303	1559
53	227	421	631	857	1087	1307	1567
59	229	431	641	859	1091	1319	1571
61	233	433	643	863	1093	1321	1579
67	239	439	647	877	1097	1327	1583
71	241	443	653	881	1103	1361	1597
73	251	449	659	883	1109	1367	1601
79	257	457	661	887	1117	1373	1607
83	263	461	673	907	1123	1381	1609
89	269	463	677	911	1129	1399	1613
97	271	467	683	919	1151	1409	1619
101	277	479	691	929	1153	1423	1621
103	281	487	701	937	1163	1427	1627
107	283	491	709	941	1171	1429	1637
109	293	499	719	947	1181	1433	1657
113	307	503	727	953	1187	1439	1663
127	311	509	733	967	1193	1447	1667
131	313	521	739	971	1201	1451	1669
137	317	523	743	977	1213	1453	1693

续 表

p	p	p	p	p	p	p	p
1697	1973	2221	2459	2719	2999	3299	3541
1699	1979	2237	2467	2729	3001	3301	3547
1709	1987	2239	2473	2731	3011	3307	3557
1721	1993	2243	2477	2741	3019	3313	3559
1723	1997	2251	2503	2749	3023	3319	3571
1733	1999	2267	2521	2753	3037	3323	3581
1741	2003	2269	2531	2767	3041	3329	3583
1747	2011	2273	2539	2777	3049	3331	3593
1753	2017	2281	2543	2789	3061	3343	3607
1759	2027	2287	2549	2791	3067	3347	3613
1777	2029	2293	2551	2797	3079	3359	3617
1783	2039	2297	2557	2801	3083	3361	3623
1787	2053	2309	2579	2803	3089	3371	3631
1789	2063	2311	2591	2819	3109	3373	3637
1801	2069	2333	2593	2833	3119	3389	3643
1811	2081	2339	2609	2837	3121	3391	3659
1823	2083	2341	2617	2843	3137	3407	3671
1831	2087	2347	2621	2851	3163	3413	3673
1847	2089	2351	2633	2857	3167	3433	3677
1861	2099	2357	2647	2861	3169	3449	3691
1867	2111	2371	2657	2879	3181	3457	3697
1871	2113	2377	2659	2887	3187	3461	3701
1873	2129	2381	2663	2897	3191	3463	3709
1877	2131	2383	2671	2903	3203	3467	3719
1879	2137	2389	2677	2909	3209	3469	3727
1889	2141	2393	2683	2917	3217	3491	3733
1901	2143	2399	2687	2927	3221	3499	3739
1907	2153	2411	2689	2939	3229	3511	3761
1913	2161	2417	2693	2953	3251	3517	3767
1931	2179	2423	2699	2957	3253	3527	3769
1933	2203	2437	2707	2963	3257	3529	3779
1949	2207	2441	2711	2969	3259	3533	3793
1951	2213	2447	2713	2971	3271	3539	3797

续 表

p	p	p	p	p	p	p	p
3803	3943	4099	4253	4421	4567	4723	4903
3821	3947	4111	4259	4423	4583	4729	4909
3823	3967	4127	4261	4441	4591	4733	4919
3833	3989	4129	4271	4447	4597	4751	4931
3847	4001	4133	4273	4451	4603	4759	4933
3851	4003	4139	4283	4457	4621	4783	4937
3853	4007	4153	4289	4463	4637	4787	4943
3863	4013	4157	4297	4481	4639	4789	4951
3877	4019	4159	4327	4483	4643	4793	4957
3881	4021	4177	4337	4493	4649	4799	4967
3889	4027	4201	4339	4507	4651	4801	4969
3907	4049	4211	4349	4513	4657	4813	4973
3911	4051	4217	4357	4517	4663	4817	4987
3917	4057	4219	4363	4519	4673	4831	4993
3919	4073	4229	4373	4523	4679	4861	4999
3923	4079	4231	4391	4547	4691	4871	
3929	4091	4241	4397	4549	4703	4877	
3931	4093	4243	4409	4561	4721	4889	

习 题

1. 证明当任意一个整数 a 的个位数能被 2 除尽时，则这个整数是 2 的倍数.

2. 证明当任意一个整数 a 的个位数能被 5 除尽时，则这个整数是 5 的倍数.

3. 证明任意一个奇数 a 的平方减 1 都是 8 的倍数.

4. 证明任意四个连续整数的乘积加 1 必定是一个平方数.

5. 证明当 a 是整数时，$a(a-1)(2a-1)$ 是 6 的倍数.

6. 证明当 a 是奇数时，$a(a^2-1)$ 是 24 的倍数.

7. 证明一个整数 a 若不能被 2 和 3 整除，则 a^2+23 必能被 24 除尽.

8. 用分解素因数的方法求最大公因数:

(i) 48, 84, 120.

(ii) 360, 810, 1260, 3150.

9. 用辗转相除法求最大公因数:

(i) 51425, 13310.

(ii) 353430, 530145, 165186.

(iii) 81719, 52003, 33649, 30107.

10. 求下列各数的最小公倍数:

(i) 391, 493.

(ii) 209, 665, 4025.

(iii) 1965, 1834, 30261, 55020.

11. 若 a, b, n 是正整数，证明:

(i) $(a^n, b^n)=(a, b)^n$.

(ii) $(na, nb)=n(a, b)$.

12. 利用上一题关于最大公因数的性质求下列最大公因数:

(i) 216, 64, 1000.

(ii) 24000, 36000, 144000.

13. 证明: 假设 a 和 b 是任意两个正整数，并且

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k},\quad \alpha_i\geqslant 0,\quad i=1, 2, \cdots, k,$$

$$b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k},\quad \beta_i\geqslant 0,\quad i=1, 2, \cdots, k,$$

这里 $p_1, \cdots, p_k$ 为不同的素因数. 又假设 γ_i 是 α_i 和 β_i 中较小的数，δ_i 是 α_i 和 β_i 中较大的数，则

$$(a, b)=p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_k^{\gamma_k},$$

$$\{a, b\}=p_1^{\delta_1}p_2^{\delta_2}\cdots p_k^{\delta_k}.$$

14. 有一间长方形的屋子长 5.25 米，宽 3.25 米，现用方砖

铺地，要恰好铺满整个屋子，问所用方砖最大边长是多少？

15. 一块长方体的木料长 3 尺 5 寸 7 分，宽 1 尺另 5 分，厚 8 寸 4 分，要把它锯成同样大小的方木块，木块的体积要最大，问木块的边长是多少？

16. 甲、乙、丙三个班的学生人数分别是 54 人，48 人和 72 人，现要在各班内分别组织体育锻练小组，但各小组的人数要相同，问锻练小组的人数最多是多少？这时甲、乙、丙三班各有多少个小组？

17. 一箱手榴弹，设每颗手榴弹的重量都是超过一斤的整数斤，去掉箱子重量后净重 201 斤，然后拿出若干颗手榴弹后，净重 183 斤，求证每颗手榴弹的重量为 3 斤.

18. 金星和地球在某一时刻相对于太阳处于某一确定位置，已知金星绕太阳一周为 225 日，地球绕太阳一周为 365 日，问这两个行星至少经多少日仍同时回到原来位置上？

19. 设计一种底面为正方形的包装箱，装运四种不同规格的象棋，每种棋盒底面都是正方形，边长分别是 21 厘米、12 厘米、14 厘米和 10.5 厘米，要使包装箱不论装运那一种规格的象棋都能铺满底面，问包装箱底面的边长至少为多少厘米？

20. 团体操在表演过程中，要求在队伍变换成 10 行、15 行、18 行、24 行时，队形都能成为长方形. 问参加团体操表演的最少需要有多少人？

21. 有甲、乙、丙、丁四个齿轮互相啮合，齿数分别为 84, 36, 60 和 48. 问在传动过程中同时啮合的各齿到下次再同时啮合时，各齿轮分别转过多少圈？

22. 求下列各数的标准分解式：

(i) 16500.

(ii) 1452990.

23. 假若 n 和 A 是正整数，并且 $\sqrt[n]{A}$ 不是整数. 证明

$\sqrt[n]{A}$ 一定不是有理分数。(有理分数就是不等于整数的分数，也就是分数中分子不能被分母整除的那些分数。)

24. 假设 n 次代数方程

$$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

的系数 $a_1, a_2, \cdots, a_n$ 都是整数。如果它有有理数的根，证明这个根一定是整数。

25. 证明：当 n 通过一切自然数时，形如 $4n-1$ 的数中包含有无限多个素数。

26. 试造一个 100 以内的素数表。

27. 求下列最大公因数：

(i) 435785667，131901878。

(ii) 15959989，7738。

28. 求下列各数的标准分解式：

(i) 174530187。

(ii) 710352035484。

(iii) 40528613317500。

29. 请证明 $F_5 = 2^{32} + 1$ 不是素数。

第二章　数的进位法

§1. 进位的概念

在生产劳动和日常生活中，数的进位制有很多种．我们最常用、最熟悉的是十进制，例如十寸为一尺，十尺为一丈，十两为一斤等．但是，日常生活中，并不都是采用十进制的．例如：一年等于十二个月，是十二进制；一小时等于六十分，一分等于六十秒，是六十进制；中药店的秤一斤等于十六两，是十六进制；鞋是以双计算的，一双等于二只，是二进制．

§2. 数的十进制

由于我们最常用、最熟悉的是十进制，所以数的写法平常是用十进位的．在十进制计数方法中共有十个不同的数字符号 0，1，2，3，4，5，6，7，8，9，而且由低位向高位是“逢十进一”的，同一个数所在的位数相差一位，其值就有十倍之差．在十进制中的数 1 就是一、10 就是十、100 就是一百．又 10 是 1 的十倍，而 100 是 10 的十倍．在十进制中由 0，1，2，3，4，5，6，7，8，9 这十个数字符号，加上正负号、小数点等就可以构成一个数．考察 1977 这个数，通常读为一千九百七十七，说得详细点，是一个一千加上九个一百加上七个十再加上七．用数学公式表达如下

$$1977 = 1 \times 10^3 + 9 \times 10^2 + 7 \times 10 + 7.$$

在十进制中任一个正整数N都能够写成

$$N = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_3 \times 10^3 + a_2 \times 10^2 + a_1 \times 10 + a_0 \qquad (2.1)$$

其中 $0 \leqslant a_i \leqslant 9$，而 i 是 0 到 n 中的任一个整数.

例如将 2345 写成等式(2.1)的形式时，则当 $i \geqslant 4$ 时有 $a_i = 0$，又有 $a_3 = 2$，$a_2 = 3$，$a_1 = 4$，$a_0 = 5$，即

$$2345 = 2 \times 10^3 + 3 \times 10^2 + 4 \times 10 + 5.$$

在十进制中，由于利用 0，1，2，3，4，5，6，7，8，9 这十个数字符号就可以表示出任意大小的数，因而十进制被普遍应用，似乎没有必要搞其它进位制，事实上在电子数字计算机出现以前，除了少数数学家以外，确实没有人考虑其他进位制．但是，随着电子数字计算机的出现和发展，除十进制外，其他进位制的作用愈来愈显著了.

§3. 数的二进制

电子数字计算机中数是采用二进制表示的．在二进制计数方法中，只有二个数字符号 0，1，而且由低位向高位是"逢二进一"的，同一个数所在的位数相差一位，其值就有二倍之差．所以，在二进制中的数 0 就是零，1 就是一，10 就是二，100 就是四，1000 就是八，10000 就是十六，100000 就是三十二，1000000 就是六十四，10000000 就是一百二十八，等等．由于在二进制中 10 就是二，1 就是一，所以在二进制中 $11 = 10 + 1$ 等于二加一也就是三．由于在二进制中 100 就是四，10 就是二，所以在二进制中 $111 = 100 + 10 + 1$ 等于四加二再加一，也就是七．对于同样由 1111 这四个数字符号所组成的数在十进制和二进制中，它们所表示的值是不同的．在十进制中 1111 就是一千一百一十一，但在二进制中 $1111 = 1000 + 100 + 10 + 1$ 却是八加四加二再加一，也就是十五．以后当 g 是正整数而 g 不等于 10 时，我们将用 $(a)_g$ 来表示 a 是用 g 进位法写的，因此 $(a)_2$ 是表示 a 是用二进位法写的．为了方便起见，当 a 是用十进位法写时，我们还用平常的写法，也就

是 a. 所以以后没有加括号的数，都表示是用十进位法写的.

在电子计算机中采用二进制，是因为这种进位制具有下面的优点：

一、我们知道，二进制数只有 0，1 两个数字符号，十进制数却有 0，1，2，3，4，5，6，7，8，9 十个数字符号. 电子计算机不可能象人一样，一眼就识别这十个符号. 在计算机内只能用物理元件的不同稳定状态来表征这些不同符号. 因此，对于一个十进制数就需要一个具有十种不同稳定状态的物理元件，对于一个二进制数只要一个具有二种不同稳定状态的物理元件即可. 显然在自然界里，后一种物理元件是较普遍存在的，也就是说是容易实现的. 例如电灯的"亮"与"暗"和开关的"接通"与"断开"都是电灯和开关的两种不同稳定状态，如果用"亮"或"接通"表示 1，则"暗"或"断开"就表示 0，所以用电灯或开关就可以表示一个二进制数.

二、采用二进制，可以用较少的物理元件表示较多的数，所以采用二进制可以节省设备而使电子计算机的结构比较简单，也有利于工作可靠性的提高.

三、二进制数的四则运算和十进制数相同，因为它只有 0 和 1 两个数字符号，因此只要记住"逢二进一"的原则，就可以进行任何运算了.

§4. 十进制数和二进制数的相互换算

由于电子数字计算机中的数是采用二进制的，因此要在电子数字计算机进行运算时，必须首先把需要运算的十进制数"翻译"成二进制数输入到机器中；计算所得到的二进制数结果也必须"翻译"成十进制数再输出给人们. 因此必须掌握这两种计数制相互换算的方法.

例 1 用二进制数表示十进制的 0，1，2，3，4，5，6，7，

8，9这十个数字符号.

解 $0=(0)_2$，　$1=(1)_2$，　$2=(10)_2$，

$3=2+1=(10)_2+(1)_2=(11)_2$，

$4=(100)_2$，

$5=4+1=(100)_2+(1)_2=(101)_2$，

$6=4+2=(100)_2+(10)_2=(110)_2$，

$7=6+1=(110)_2+(1)_2=(111)_2$，

$8=(1000)_2$，

$9=8+1=(1000)_2+(1)_2=(1001)_2$.

这里介绍一种基于下表的对应关系，采用试减法来将十进制数转换成二进制数.

表1　2的乘次方表

乘次方	数值	乘次方	数值
1	2	9	512
2	4	10	1024
3	8	11	2048
4	16	12	4096
5	32	13	8192
6	64	14	16384
7	128	⋮	⋮
8	256		

例2　24化为二进制数等于什么?

解　由表1的数值那一列知道不大于24的最大数是16而 $2^4=16$. 由 $24-16=8$ 和由表1的数值那一列知道不大于8的最大数是8，而有 $2^3=8$. 由于

$$24=16+8=1\times2^4+1\times2^3+0\times2^2+0\times2+0,$$

所以　　$(24)=(11000)_2$.

例3　92化为二进制数等于什么?

解 由表 1 的数值那一列知道不大于 92 的最大数是64，而有 $2^6=64$。由$92-64=28$，再由表 1 的数值那一列知道不大于 28 的最大数是 16，而有 $2^4=16$。由 $28-16=12$，再由表 1 的数值那一列知道不大于 12 的最大数是 8，而有 $2^3=8$。由 $12-8=4$，再由表 1 的数值那一列知道不大于 4 的最大值是 4，而有 $2^2=4$。由于

$$
\begin{aligned}
92 &= 64+16+8+4=1\times 2^6+0\times 2^5 \\
&\quad +1\times 2^4+1\times 2^3+1\times 2^2+0\times 2+0,
\end{aligned}
$$

所以 $92=(1011100)_2$。

现在再介绍另外一种不用表 1 而直接将十进制数转换成二进制数的方法。设十进制数 a 为正整数，又设 a 化为二进制数为 $(b_nb_{n-1}\cdots b_1b_0)_2$，则我们有

$$a=b_n\times 2^n+b_{n-1}\times 2^{n-1}+\cdots+b_1\times 2+b_0.$$

为了求出等式右端的各系数，我们将等式两端均除以 2，得到

$$\frac{a}{2}=b_n\times 2^{n-1}+b_{n-1}\times 2^{n-2}+\cdots+b_1+\frac{b_0}{2}.$$

根据两个相等的有理数其整数部分和分数部分必分别相等的道理，我们看出 a 除以 2 后所得的余数就是 b_0。同样的道理，将 $\frac{a}{2}$ 的整数部分再除以 2，所得的余数就是 b_1。依此类推，这样就可以得到 $b_0, b_1, \cdots, b_n$，从而得到 $(b_nb_{n-1}\cdots b_1b_0)_2$。

例 4 19 化成二进制数等于什么？

解 $19\div 2=9+\frac{1}{2}$，因为除后余数是 1，故 $b_0=1$。

$9\div 2=4+\frac{1}{2}$，因为除后余数是 1，故 $b_1=1$。

$4\div 2=2+0$，因为除后余数是 0，故 $b_2=0$。

$2\div 2=1+0$，因为除后余数是 0，故 $b_3=0$。

$$1 \div 2 = \frac{1}{2}，\text{因为除后余数是 1，故 } b_4 = 1.$$

于是 19 用二进制数表示就是 $(10011)_2$.

至于二进制数转换成十进制数，方法就比较简单了，只要把它用 2 的乘次方的多项式表示，求出结果就行了.

例 5　$(10011)_2$ 化成十进制数等于什么?

解　$(10011)_2 = 1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 1 \times 2 + 1 = 19.$

例 6　$(110101)_2$ 化成十进制数等于什么?

解　$(110101)_2 = 1 \times 2^5 + 1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 0 \times 2 + 1 = 32 + 16 + 4 + 1 = 53.$

§ 5. 数的八进制

事物总是一分为二的，二进制数虽然具有上述值得被电子计算机采用的优点，但也存在有某些缺点.

二进制数的一个缺点是：人们通常使用的是十进制数，对于二进制数就很不习惯. 当然这个缺点不是主要的，多接触后也就会从不习惯转化为习惯了，何况电子数字计算机借助于计算程序都能自动实现十进制数与二进制数之间的相互转换，使用者就更不必担心不习惯了.

二进制数的另一个缺点是：表示同一个数值，采用二进制数所需的位数较多. 例如 1023 共四位，用二进制数表示是 $(1111111111)_2$，共十位，读写和观察都非常不便.

在编制计算程序及控制台的实际工作中，为了弥补这一不足，在二进制的基础上人们还采用了八进制和十六进制的表示方法，其中以八进制用得最多.

八进制具有 0，1，2，3，4，5，6，7 等八个数字符号，由

低位向高位是“逢八进一”的，同一个数所在的位数相差一位，其值就有八倍之差（以后我们将用 $(a)_8$ 来表示 a 是用八进制法写的），所以在八进制中有

$$(0)_8=0,\quad (1)_8=1,\quad (2)_8=2,\quad (3)_8=3,$$
$$(4)_8=4,\quad (5)_8=5,\quad (6)_8=6,\quad (7)_8=7,$$
$$(10)_8=8,\quad (100)_8=8^2=64,$$
$$(1000)_8=8^3=512,$$
$$(10000)_8=8^4=4096,\cdots\cdots.$$

又有

$$(11)_8=(10)_8+(1)_8=8+1=9,$$
$$(12)_8=(10)_8+(2)_8=8+2=10,$$
$$(13)_8=(10)_8+(3)_8=8+3=11,$$
$$(14)_8=(10)_8+(4)_8=8+4=12.$$

例 7 $(736)_8$ 化为十进制数等于什么？

解 $(736)_8=7\times 8^2+3\times 8+6=448+24$
$+6=478.$

例 8 $(1712)_8$ 化为十进制数等于什么？

解 $(1712)_8=1\times 8^3+7\times 8^2+1\times 8+2$
$=970.$

现在介绍一种将十进制数转换成八进制数的方法. 设十进制数 a 为正整数，又设 a 化为八进制数为 $(b_nb_{n-1}\cdots b_1b_0)_8$，则我们有

$$a=b_n\times 8^n+b_{n-1}\times 8^{n-1}+\cdots+b_1\times 8+b_0.$$

为了求出等式右端的各系数，我们将上面的等式两端均除以8，得到

$$\frac{a}{8}=b_n\times 8^{n-1}+b_{n-1}\times 8^{n-2}+\cdots+b_1+\frac{b_0}{8}.$$

根据两个相等的有理数其整数部分和分数部分必分别相等的

道理，我们看出 a 除以 8 后所得的余数就是 b_0。同样的道理将 $\frac{a}{8}$ 的整数部分再除以 8，所得的余数就是 b_1。依此类推，这样就可以得到 $b_0, b_1, \cdots, b_n$。从而得到 $(b_nb_{n-1}\cdots b_1b_0)_8$。

例 9 将 117 化为八进制数等于什么？

解 由 $\frac{117}{8}=14+\frac{5}{8}$ 得到 $b_0=5$，由 $\frac{14}{8}=1+\frac{6}{8}$ 得到 $b_1=6$，$b_2=1$，

即
$$117=(165)_8.$$

例 10 将 92 化为八进制数等于什么？

解 由 $\frac{92}{8}=11+\frac{4}{8}$ 得到 $b_0=4$，

由 $\frac{11}{8}=1+\frac{3}{8}$ 得到 $b_1=3$，$b_2=1$，

即
$$92=(134)_8.$$

如果要将一个二进制数转换成八进制数，可先将这个二进制数的数字从右向左依次将每三个数字分为一组，最后一组不够三个数字时可在前面添加 0，使成三个数字，再将每一组和八进制数中的一个数字进行转换，转换时可使用下面的式子

$$\begin{aligned}
&(0)_8=0=(0)_2=(000)_2,\\
&(1)_8=1=(1)_2=(001)_2,\\
&(2)_8=2=(10)_2=(010)_2,\\
&(3)_8=3=(11)_2=(011)_2,\\
&(4)_8=4=(100)_2,\\
&(5)_8=5=(101)_2,\\
&(6)_8=6=(110)_2,\\
&(7)_8=7=(111)_2.
\end{aligned}\tag{2.2}$$

例 11 将 $(101001)_2$ 化为八进制数。

解 第一步先将这个二进制数依次分成三个数字为一组，$(101001)_2=(101\ \ 001)_2$，然后使用(2.2)式中的式子

$(101)_2=(5)_8$，$(001)_2=(1)_8$，

即得 $$(101001)_2=(51)_8.$$

例 12 将$(111001101010)_2$化为八进制数.

解 第一步先将这个二进制数依次分成三个数字为一组 $(111001101010)_2=(111\ \ 001\ \ 101\ \ 010)_2$ 然后使用(2.2)式中的式子

$$(111)_2=(7)_8,\quad (001)_2=(1)_8,$$
$$(101)_2=(5)_8,\quad (010)_2=(2)_8,$$

即得

$$(111001101010)_2=(7152)_8.$$

如果要将一个八进制数转换成二进制数，可以将这个八进制数的数字依次和每三个数字为一组的二进制数进行转换，转换时还可以使用(2.2)式中的式子.

例 13 将$(573)_8$化为二进制数.

解 使用(2.2)中的式子，我们有

$$(5)_8=(101)_2,$$
$$(7)_8=(111)_2,$$
$$(3)_8=(011)_2,$$

即得

$$(573)_8=(101111011)_2.$$

例 14 将$(2175)_8$化为二进制数.

解 使用(2.2)中的式子，我们有

$$(2)_8=(010)_2,\quad (1)_8=(001)_2,$$
$$(7)_8=(111)_2,\quad (5)_8=(101)_2,$$

即得

$$(2175)_8=(010001111101)_2=(10001111101)_2.$$

§ 6. 二进制的加法和乘法

我们在小学里都学习过乘法九九口诀，要背熟这个九九口诀，实在是一件很辛苦的事情. 但一旦熟记了这个口诀，做起乘法和除法来就会得心应手.

与此相同，在二进制中进行加减乘除四则运算时，我们也要使用加法与乘法的运算规则. 首先，我们介绍加法运算规则，如下表所示:

$$(0)_2+(0)_2=(0)_2$$
$$(0)_2+(1)_2=(1)_2$$
$$(1)_2+(0)_2=(1)_2$$
$$(1)_2+(1)_2=(10)_2$$

下面是使用此规则进行加法运算的例题.

$$\begin{array}{r}(10)_2\\ +\ (11)_2\\ \hline (101)_2\end{array},\quad \begin{array}{r}(101)_2\\ +\ (10)_2\\ \hline (111)_2\end{array},\quad \begin{array}{r}(11)_2\\ +\ (11)_2\\ \hline (110)_2\end{array},$$

$$\begin{array}{r}(101)_2\\ +\ (11)_2\\ \hline (1000)_2\end{array},\quad \begin{array}{r}(110)_2\\ +\ (101)_2\\ \hline (1011)_2\end{array},\quad \begin{array}{r}(1000)_2\\ +\ (111)_2\\ \hline (1111)_2\end{array},$$

$$\begin{array}{r}(1001)_2\\ +\ (1101)_2\\ \hline (10110)_2\end{array},\quad \begin{array}{r}(1111)_2\\ +\ (110)_2\\ \hline (10101)_2\end{array},\quad \begin{array}{r}(1111)_2\\ +\ (111)_2\\ \hline (10110)_2\end{array}.$$

现在我们已经熟悉了二进制的加法运算，接下去，我们就要讲述二进制的乘法运算. 在二进制中与 $(0)_2$ 相乘时，和十进制相同，乘法运算规则如下表所示:

$$
\begin{array}{|l|}
\hline
(0)_2 \times (0)_2 = (0)_2 \\
(0)_2 \times (1)_2 = (0)_2 \\
(1)_2 \times (0)_2 = (0)_2 \\
(1)_2 \times (1)_2 = (1)_2 \\
\hline
\end{array}
$$

看一下下面所举的例题，就可完全掌握其乘法方法.

$$
\begin{array}{r}
(1\,1)_2 \\
\times \quad (1)_2 \\
\hline
(1\,1)_2
\end{array},
\qquad
\begin{array}{r}
(1\,0\,1)_2 \\
\times \quad (1)_2 \\
\hline
(1\,0\,1)_2
\end{array},
\qquad
\begin{array}{r}
(1\,1\,1)_2 \\
\times \quad (1)_2 \\
\hline
(1\,1\,1)_2
\end{array},
$$

$$
\begin{array}{r}
(1\,1)_2 \\
\times \quad (1\,0)_2 \\
\hline
(0\,0)_2 \\
+\ (1\,1\,0)_2 \\
\hline
(1\,1\,0)_2
\end{array},
\qquad
\begin{array}{r}
(1\,0\,1)_2 \\
\times \quad (1\,0)_2 \\
\hline
(0\,0\,0)_2 \\
+\ (1\,0\,1\,0)_2 \\
\hline
(1\,0\,1\,0)_2
\end{array},
\qquad
\begin{array}{r}
(1\,0\,1)_2 \\
\times \quad (1\,1)_2 \\
\hline
(1\,0\,1)_2 \\
+\ (1\,0\,1\,0)_2 \\
\hline
(1\,1\,1\,1)_2
\end{array},
$$

$$
\begin{array}{r}
(1\,1\,0\,0)_2 \\
\times \quad (1\,0)_2 \\
\hline
(0\,0\,0\,0)_2 \\
+\ (1\,1\,0\,0\,0)_2 \\
\hline
(1\,1\,0\,0\,0)_2
\end{array},
\qquad
\begin{array}{r}
(1\,1\,1\,0)_2 \\
\times \quad (1\,1)_2 \\
\hline
(1\,1\,1\,0)_2 \\
+\ (1\,1\,1\,0\,0)_2 \\
\hline
(1\,0\,1\,0\,1\,0)_2
\end{array}.
$$

§7. 二进制的减法

在说明减法运算之前，让我们先来举减法运算方法的例子.

$$
\begin{array}{r}
(1\,1)_2 \\
- \quad (1)_2 \\
\hline
(1\,0)_2
\end{array},
\qquad
\begin{array}{r}
(1\,0\,1)_2 \\
- \quad (1)_2 \\
\hline
(1\,0\,0)_2
\end{array},
\qquad
\begin{array}{r}
(1\,1\,1)_2 \\
- \quad (1)_2 \\
\hline
(1\,1\,0)_2
\end{array},
$$

$$\begin{array}{r}(110)_2\\ -\quad(10)_2\\ \hline (100)_2\end{array},\qquad \begin{array}{r}(10)_2\\ -\quad(1)_2\\ \hline (1)_2\end{array},\qquad \begin{array}{r}(100)_2\\ -\quad(1)_2\\ \hline (11)_2\end{array},$$

$$\begin{array}{r}(100)_2\\ -\quad(11)_2\\ \hline (1)_2\end{array},\qquad \begin{array}{r}(101)_2\\ -\quad(11)_2\\ \hline (10)_2\end{array},\qquad \begin{array}{r}(110)_2\\ -\quad(11)_2\\ \hline (11)_2\end{array}.$$

正如您所看到的，减法没有象加法那样容易，当遇到"0－1"的情况时，就需要向上位"借"．在二进制中，$(10)_2 = (1)_2 + (1)_2$，所以从上位借来的"1"应是 $(1)_2 + (1)_2$．二进制的减法，似乎比加法和乘法麻烦，不过在电子计算机中也有使其简化的方法，这便是使用补数．

我们在十进制数字的计算中，如减 9（或 99）之类的数字时，往往先减掉 10（或 100），然后再加上 1，这样的简化方法自古以来就在心算中经常使用着．

由于 $10 - 7 = 3$，所以我们说 7 的补数是 3．由于 $100 - 89 = 11$，所以我们说 89 的补数是 11．如果 a 是一个正整数而 n 是一个非负整数并有 $10^n < a < 10^{n+1}$，则我们说 a 的补数是 $10^{n+1} - a$．

由 12 减去 7 时 $(12 - 7)$，可首先求出减数 7 的补数．由于 $10 - 7 = 3$，所以 7 的补数是 3．然后被减数 12 加上减数 7 的补数 3 得 15（即 $12 + 3 = 15$），再减去 10 而得到 5，这就是 12 减去 7 时的答案．

设 a 和 b 都是正整数，$a > b$ 而 $10^n < b < 10^{n+1}$，其中 n 是一个非负整数．我们可以将 $a - b$ 变换成如下的形式：

被减数 a ＋ 减数 b 的补数-10^{n+1}

即

$$a - b = a + (10^{n+1} - b) - 10^{n+1}.$$

例如

$$127 - 74 = 127 + 26 - 100 = 53,$$
$$369 - 87 = 369 + 13 - 100 = 282,$$
$$1025 - 787 = 1025 + 213 - 1000 = 238,$$
$$10127 - 9974 = 10127 + 26 - 10000 = 153.$$

二进制的补数与十进制的补数有些相似. 由于$(10)_2 - (1)_2 = (1)_2$, 所以我们说$(1)_2$的补数是$(1)_2$. 由于$(100)_2 - (10)_2 = (10)_2$, 所以$(10)_2$的补数是$(10)_2$. 由于$(100)_2 - (11)_2 = (1)_2$, 所以$(11)_2$的补数是$(1)_2$. 如果$n \geqslant 3$而$(a_1a_2\cdots a_n)_2$是一个二进制数, 则我们说$(a_1a_2\cdots a_n)_2$的补数是

$$(100\cdots0)_2 - (a_1a_2\cdots a_n)_2,$$

其中$(100\cdots0)_2$是由一个1和n个0所构成的. 当$n \geqslant 3$时为了较快地求出$(a_1a_2\cdots a_n)_2$的补数, 我们可用下面方法来求补数.

(1) 当$a_n = 1$时, 除a_n不变外, 在$a_1, a_2, \cdots a_{n-1}$中所有a_i是0的都变成1, 而所有a_i是1的都变成0. 由这种方法所得到的二进制数就是$(a_1a_2\cdots a_n)_2$的补数.

例如$(101)_2$的补数是$(011)_2 = (11)_2$. $(11)_2$的补数是$(01)_2 = (1)_2$. $(1001)_2$的补数是$(0111)_2 = (111)_2$. $(1011)_2$的补数是$(0101)_2 = (101)_2$.

(2) 当$a_n = 0$时, 在$(a_1a_2\cdots a_n)_2$中从右往左看, 则在出现1以前所有的0及其第一次出现的1都不变, 而后各数遇0变成1, 遇1则变成0. 用这种方法所得到的二进制数就是$(a_1a_2\cdots a_n)_2$的补数.

例如$(110)_2$的补数是$(010)_2 = (10)_2$, 而$(1100)_2$的补数是$(0100)_2 = (100)_2$.

下面, 我们利用补数来进行二进制减法运算.

例 15 求 $(1101)_2-(1011)_2=?$

解 先求 $(1011)_2$ 的补数，得到 $(0101)_2=(101)_2$，然后将被减数 $(1101)_2$ 加上补数而得到

$$\begin{array}{r} (1101)_2 \\ +\quad (101)_2 \\ \hline (10010)_2 \end{array},$$

然后再减去 $(10000)_2$，便可求得此减法的答案

$$\begin{array}{r} (10010)_2 \\ -(10000)_2 \\ \hline (10)_2 \end{array}.$$

例 16 求 $(1011)_2-(101)_2=?$

解 先求 $(101)_2$ 的补数，得到 $(011)_2=(11)_2$，然后将被减数 $(1011)_2$ 加上补数而得到

$$\begin{array}{r} (1011)_2 \\ +\quad (11)_2 \\ \hline (1110)_2 \end{array},$$

然后再减去 $(1000)_2$，便获得此减法的答案

$$\begin{array}{r} (1110)_2 \\ -(1000)_2 \\ \hline (110)_2 \end{array}.$$

例 17 求 $(11101)_2-(1011)_2=?$

解 先求 $(1011)_2$ 的补数，得到 $(0101)_2=(101)_2$，然后将被减数 $(11101)_2$ 加上补数而得到

$$\begin{array}{r} (11101)_2 \\ +\quad (101)_2 \\ \hline (100010)_2 \end{array},$$

然后再减去$(10000)_2$，便获得此减法的答案

$$\begin{array}{r} (100010)_2 \\ -\quad (10000)_2 \\ \hline (10010)_2 \end{array}.$$

§8. 二进制的除法

二进制中的除法运算，首先是比较二数的大小，然后由减法运算来求商.

$(1001)_2 \div (11)_2 = ?$

现在，让我们用二进制的普通除法运算来求上式的商，得

$$\begin{array}{r} (11)_2 \\ (11)_2 \overline{\big)\ (1001)_2} \\ -(110)_2 \\ \hline (11)_2 \\ -(11)_2 \\ \hline (0)_2 \end{array}.$$

在计算上式前，我们首先要比较被除数$(1001)_2$的前二位数(从左向右，在这里即10)与除数$(11)_2$(在这里即11)的大小，因为$10 < 11$，所以先用$(100)_2$来被$(11)_2$除.

下面，再举一个例子

$$\begin{array}{r} (11)_2 \\ (101)_2 \overline{\big)\ (1111)_2} \\ -(1010)_2 \\ \hline (101)_2 \\ -(101)_2 \\ \hline (0)_2 \end{array}.$$

但是，除法可以用减法来代替. 例如100被10除，这就意味着在100中包含有多少个10. 所以，从100中一次又一

次地减去 10，直到减完，其减去的次数便是商.

在二进制中，除法用减法代替，而减法则又可使用补数来求答案.

例 18 求 $(1111)_2 \div (101)_2 = ?$

解 首先求除数 $(101)_2$ 的补数，得到 $(011)_2 = (11)_2$，然后将被除数 $(1111)_2$ 加上补数 $(11)_2$ 而得到

$$\begin{array}{r} (1\,1\,1\,1)_2 \\ +\quad (1\,1)_2 \\ \hline (1\,0\,0\,1\,0)_2 \end{array},$$

然后再减去 $(1000)_2$，便获得第一次减去除数后的余数，即

$$\begin{array}{r} (1\,0\,0\,1\,0)_2 \\ -\quad (1\,0\,0\,0)_2 \\ \hline (1\,0\,1\,0)_2 \end{array},$$

然后再将余数 $(1010)_2$ 加上补数 $(11)_2$ 再减去 $(1000)_2$，便获得第二次减去除数后的余数，即

$$\begin{array}{r} (1\,0\,1\,0)_2 \\ +\quad (1\,1)_2 \\ \hline (1\,1\,0\,1)_2 \\ -(1\,0\,0\,0)_2 \\ \hline (1\,0\,1)_2 \end{array},$$

然后再将余数 $(101)_2$ 加上补数 $(11)_2$ 再减去 $(1000)_2$，便获得第三次减去除数后的余数

$$\begin{array}{r} (1\,0\,1)_2 \\ +\quad (1\,1)_2 \\ \hline (1\,0\,0\,0)_2 \\ -(1\,0\,0\,0)_2 \\ \hline (0)_2 \end{array}.$$

不难看出，因为总共减了三次刚好减完，其商是3．最后将十进制数3变换成二进制数而得$(11)_2$，所以

$$(1111)_2 \div (101)_2 = (11)_2.$$

例 19 求$(101101)_2 \div (1111)_2 = ?$

解 首先求除数$(1111)_2$的补数，得到$(0001)_2 = (1)_2$，然后将被除数$(101101)_2$加上补数$(1)_2$再减去$(10000)_2$，便获得第一次减去除数后的余数，即

$$\begin{array}{r} (101101)_2 \\ +\qquad (1)_2 \\ \hline (101110)_2 \\ -\ (10000)_2 \\ \hline (11110)_2 \end{array},$$

然后再将余数$(11110)_2$加上补数$(1)_2$再减去$(10000)_2$，便获得第二次减去除数后的余数，即

$$\begin{array}{r} (11110)_2 \\ +\qquad (1)_2 \\ \hline (11111)_2 \\ -(10000)_2 \\ \hline (1111)_2 \end{array},$$

然后再将余数$(1111)_2$加上补数$(1)_2$再减去$(10000)_2$，便获得第三次减去除数后的余数，即

$$\begin{array}{r} (1111)_2 \\ +\qquad (1)_2 \\ \hline (10000)_2 \\ -(10000)_2 \\ \hline (0)_2 \end{array}.$$

不难看出，因为总共减了三次刚好减完，其商是3，最后

将十进制数 3 变换成二进制数而得 $(11)_2$, 所以

$$(101101)_2 \div (1111)_2 = (11)_2.$$

注意：小数也能用二进制(或八进制)表示，其原则也是“逢二进一”(或“逢八进一”)，而相互换算和四则运算都相似于整数时的情况. 由于数论主要是研究整数的性质，所以关于这方面我们不讲. 在笔算时，对于二进制中的数，如采用惯用的减法和除法运算，当遇到“0 − 1”的情况时而向上位借“1”似乎比使用补数方法运算起来简单，但是在电子计算机中，这样做将变得非常麻烦，所以在电子计算机中都采用了使用补数的方法，也就是说，由于使用了补数，减法和除法实质上都由加法来计算，从而使电子计算机的构造大大地简化了.

习　　题

1. 把下列各十进制数化为二进制数：

(i) 420,　　(ii) 2640.

2. 把下列各二进制数化为十进制数：

(i) $(111111)_2$,　　(ii) $(11100001)_2$.

3. 把下列各十进制数化为八进制数：

(i) 420,　　(ii) 2640.

4. 把下列各八进制数化为十进制数：

(i) $(256)_8$,　　(ii) $(11300)_8$.

5. 把下列各二进制数化为八进制数：

(i) $(101101101)_2$,　　(ii) $(101011001101001)_2$.

6. 把下列各八进制数化为二进制数：

(i) $(401)_8$,　　(ii) $(1270)_8$.

7. 求下列各二进制数的加法运算结果：

(i) $(1001)_2 + (101)_2 + (1111)_2 + (111)_2 = ?$

(ii) $(101011)_2 + (10011)_2 + (1111)_2 = ?$

8. 求下列各二进制的乘法运算结果:

(i) $(111)_2 \times (101)_2 = ?$

(ii) $(1001)_2 \times (111)_2 \times (101)_2 = ?$

9. 求下列各二进制的减法运算结果:

(i) $(1010111)_2 - (11001)_2 - (11110)_2 = ?$

(ii) $(10110001)_2 - (1101100)_2 - (11110)_2 = ?$

10. 求下列各二进制数的除法运算结果:

(i) $(1100011)_2 \div (100001)_2 = ?$

(ii) $(110001)_2 \div (111)_2 = ?$

第三章　一部分不定方程

伟大的革命导师马克思从无产阶级革命斗争的需要出发，十分注意研究自然科学．在几十年间，他对于一部分不定方程作了不少研究．他曾经解答了下面的题目：（《马克思数学手稿》）

例如有 30 个人，其中有男人，女人和小孩，在一家小饭馆里共花了 50 先令；每个男人花 3 先令，每个女人 2 先令，每个小孩 1 先令；问男人，女人和小孩各有多少？

设用 x, y, z 分别代表男人、女人和小孩的个数，就得到下面的方程

$$x + y + z = 30, \tag{1}$$

$$3x + 2y + z = 50, \tag{2}$$

由（2）式减去（1）式就得到

$$2x + y = 20. \tag{3}$$

我们要解决这个问题，就是要求出（3）式的非负整数解，但是（3）式不过是二元一次不定方程的一个具体的例子，所谓二元一次不定方程的一般形式是

$$ax + by = c, \tag{4}$$

其中 a, b, c 都是整数．在这一章中我们的主要目的是讨论二元一次不定方程有整数解的条件及其解法．

§1. 一元不定方程

我们先来讨论一元一次不定方程

$$a_1x + a_0 = 0. \tag{5}$$

这里我们假设 a_1 和 a_0 都是整数，很明显，(5) 式的解是

$$x = -\frac{a_0}{a_1},$$

只有在 a_0 能够被 a_1 整除的时候，它才是整数，由此可知，(5) 式不是随时都有整数解的．例如

$$3x - 27 = 0 \text{ 和 } 5x = 21$$

这二个方程中，第一个方程具有整数解 $x = 9$，而第二个方程就不可能有整数解．

在次数高于一的不定方程中，我们也遇到同样的情形：二次方程

$$x^2 + x - 2 = 0$$

具有整数解 $x_1 = 1$，$x_2 = -2$；二次方程

$$x^2 - 4x + 2 = 0$$

就不可能有整数解，因为它只有二个解，其中的一个解是 $2 + \sqrt{2}$，另外的一个解是 $2 - \sqrt{2}$，而这二个解都是无理数．

设 $n \geqslant 2$，而 n，a_0，a_1，$\cdots$，a_n 都是整数．关于求出整数系数的 n 次方程

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \tag{6}$$

的整数解，这个问题是很容易解决的．事实上，设 $x = \alpha$ 是 (6) 式的整数解，那么

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

$$a_0 = -\alpha(a_n\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1). \tag{7}$$

从 a_1，$\cdots$，a_n 和 α 都是整数和从 (7) 式中可以看出，a_0 能被 α 除尽；由此可知 (6) 式的每一个整数解都是 (6) 式中的 a_0 的因数．因此要求出 (6) 式的整数解就应从 a_0 的因数中去挑选出那些整数，它能够整除 a_0，并使 (6) 式成立，这些整数就是 (6) 式的整数解．例如方程

$$x^{10} + x^7 + 2x^3 + 2 = 0$$

中的 $a_0=2$, 2 的因数共有四个，即 1，-1，2 和 -2，其中只有 -1 是这个方程的解，而 1，2，-2 都不是这个方程的解．由此可知，这个方程具有唯一的整数解 $x=-1$．又例如方程

$$x^6-x^5+3x^4+x^2-x+3=0$$

中的 $a_0=3$, 3 的因数共有四个，即 1，-1，3 和 -3，但是由于这四个整数都不是这个方程的解．因此这个方程不可能有整数解．

§2. 二元一次不定方程

我们将讨论二元一次不定方程

$$ax+by=c. \tag{8}$$

这里 a 和 b 是零以外的整数，而 c 是任意的整数．因为所求的 x, y 可以是正整数或负整数，所以我们可以只讨论 a, b 都是正整数的情形．我们首先讨论 $c=0$ 时的情形，即

$$ax+by=0. \tag{9}$$

如果 a 和 b 的最大公因数是 d，而 $d>1$，即 $(a,b)=d>1$，则可用 d 来除 (9) 式，这样 x, y 的系数就变成互素之数．所以我们可设 $(a,b)=1$．解这个方程，就得到

$$x=-\frac{by}{a}.$$

很明显，当 y 被 a 整除时，在这种情形也只有在这种情形，(9) 式才具有整数解．由于一切整数 y 是 a 的倍数时，都可以表示成

$$y=at,$$

这里 t 可以取任意整数值 $(t=0,\pm1,\pm2,\cdots)$，将 $y=at$ 代入 $x=-\frac{by}{a}$，则有

$$x = -\frac{bat}{a} = -bt.$$

于是我们得到(9)式的一切整数解的公式

$$x = -bt, \quad y = at, \quad (t = 0, \pm 1, \pm 2, \cdots).$$

当 $c \neq 0$ 而 c 是一个负整数时，则可用 -1 乘(8)式，这样(8)式右边就变成正整数了．当(8)式右边是正整数时，则因所求的 x, y 可以是正整数或负整数，所以我们可以只讨论 a, b 也都是正整数的情形．我们将假定 a 和 b 是互素的．事实上，如果 a 和 b 的最大公因数 $d = (a, b) > 1$，则等式

$$a = a_1 d, \quad b = b_1 d, \quad (a_1, b_1) = 1$$

成立，因而(8)式就具有这样的形式

$$d(a_1 x + b_1 y) = c. \tag{10}$$

所以只有在 c 能被 d 整除时，(8)式才能够具有整数解，也就是说当 a 和 b 的最大公因数 d 不能够整除 c 时，(8)式没有整数解．当 $d|c$ 时，设 $c = c_1 d$，则由(10)式有

$$a_1 x + b_1 y = c_1, \quad (a_1, b_1) = 1,$$

所以对于(8)式来说，我们可以假设 $(a, b) = 1$.

引理 1 如果 a 和 b 是二个互素的正整数，则一定存在有二个整数 x, y 使得

$$ax + by = 1.$$

证 本引理的证明见习题 8.

现在我们举些具体例子来说明，怎样来求这二个整数 x 和 y.

例 1 因 $(36, 83) = 1$，故由引理 1 一定有二个整数 x, y 能使

$$36x + 83y = 1$$

成立，求 x, y.

解 由于

$$83 = 2 \times 36 + 11, \quad 36 = 3 \times 11 + 3,$$
$$11 = 3 \times 3 + 2, \quad 3 = 2 + 1,$$

而得

$$\begin{aligned} 1 &= 3 - 2 = 3 - (11 - 3 \times 3) = 4 \times 3 - 11 \\ &= 4 \times (36 - 3 \times 11) - 11 = 4 \times 36 - 13 \times 11 \\ &= 4 \times 36 - 13 \times (83 - 2 \times 36) \\ &= 30 \times 36 - 13 \times 83 \\ &= 36 \times 30 - 83 \times 13, \end{aligned}$$

故

$$x = 30, \qquad y = -13.$$

例 2 因 $(72,157) = 1$，故由引理 1 一定有二个整数 x，y 能使

$$72x + 157y = 1$$

成立，求 x，y.

解 由于

$$157 = 2 \times 72 + 13, \quad 72 = 5 \times 13 + 7,$$
$$13 = 7 + 6, \quad 7 = 6 + 1,$$

而得

$$\begin{aligned} 1 &= 7 - 6 = 7 - (13 - 7) = 2 \times 7 - 13 \\ &= 2 \times (72 - 5 \times 13) - 13 = 2 \times 72 - 11 \times 13 \\ &= 2 \times 72 - 11 \times (157 - 2 \times 72) \\ &= 24 \times 72 - 11 \times 157 = 72 \times 24 - 157 \times 11, \end{aligned}$$

故

$$x = 24, \qquad y = -11.$$

引理 2 如果 a 和 b 是二个互素的正整数，而 c 是一个整数，则一定存在有二个整数 x，y 使得

$$ax + by = c \tag{11}$$

成立.

证 由引理 1 知道存在有二个整数 s, t 使得

$$as + bt = 1$$

成立. 令 $x = sc$, $y = tc$, 则得 $ax + by = c(as + bt) = c$. 所以 (11) 式存在有整数解 x, y.

定理 1 设二元一次不定方程

$$ax + by = c \tag{8}$$

(其中 a, b, c 都是正整数而 $(a, b) = 1$) 有一组整数解 $x = x_0$, $y = y_0$, 则 (8) 式的一切整数解可以表示成

$$x = x_0 - bt, \quad y = y_0 + at, \tag{12}$$

其中 $t = 0, \pm 1, \pm 2, \pm 3, \cdots$.

证 既然 x_0, y_0 是 (8) 式的整数解, 当然满足 $ax_0 + by_0 = c$, 因此

$$a(x_0 - bt) + b(y_0 + at) = ax_0 + by_0 = c.$$

这表明 (12) 式是 (8) 式的解.

设 x', y' 是 (8) 式的任一整数解,则有 $ax' + by' = c$,减去 $ax_0 + by_0 = c$, 即得

$$a(x' - x_0) + b(y' - y_0) = 0,$$

$$a(x' - x_0) = -b(y' - y_0).$$

由上式和 $(a, b)=1$, 故由第一章引理 13 我们有 $a|(y'-y_0)$, 即 $y' = y_0 + at$, 其中 t 是一个整数. 将 $y' = y_0 + at$ 代入 $a(x' - x_0) = -b(y' - y_0)$, 即得 $x' - x_0 = -bt$, $x' = x_0 - bt$, 因此 x', y' 可表示成 (12) 式的形状. 故 (12) 式表示 (8) 式的一切整数解,因此定理 1 得证.

由定理 1 我们知道当 (8) 式有一整数解时, 它的一切整数解可由 (12) 式表示出来.

例 3 求 $111x - 321y = 75$ 的一切整数解.

解 由于

$$111 = 3 \times 37, \quad 321 = 3 \times 107,$$

$75 = 3 \times 25$ 和 $111x - 321y = 75$，而得到

$$37x - 107y = 25, \tag{13}$$

即 $111x - 321y = 75$ 的解与 (13) 式的解完全相同．今先解

$$37s + 107t = 1, \tag{14}$$

由于

$$107 = 2 \times 37 + 33, \quad 37 = 33 + 4, \quad 33 = 8 \times 4 + 1,$$

故得

$$\begin{aligned} 1 &= 33 - 8 \times 4 = 37 - 4 - 8 \times 4 = 37 - 9 \times 4 \\ &= 37 - 9 \times (37 - 33) = 9 \times 33 - 8 \times 37 \\ &= 9 \times (107 - 2 \times 37) - 8 \times 37 = 9 \times 107 \\ &- 26 \times 37 = 37 \times (-26) + 107 \times 9. \end{aligned}$$

故 (14) 式的一组整数解是 $s = -26$，$t = 9$．令 $x = 25s$，$y = -25t$，则我们由 (14) 式有

$$37x - 107y = 25(37s + 107t) = 25.$$

故 $x = 25 \times (-26) = -650$，$y = -25 \times 9 = -225$ 是 (13) 式的一组整数解．而由定理 1 我们知道 (13) 式的一切整数解可以表示成

$$x = -650 + 107t, \quad y = -225 + 37t,$$

或

$$x = -8 + 107t, \quad y = -3 + 37t.$$

(其中 $t = 0, \pm 1, \pm 2, \pm 3, \cdots$)．

例 4 求 (3) 式中的一切整数解．

解 先解 $2s + t = 1$．因为 $2 = 1 + 1$，故得 $1 = 2 - 1$．即 $s = 1$，$t = -1$ 是 $2s + t = 1$ 的一组整数解．令 $x = 20s$，$y = 20t$，则有

$$2x + y = 20(2s + t) = 20.$$

故 (3) 式的一组整数解是 $x = 20$，$y = -20$，而由定理 1 知道 (3) 式的一切整数解可以表示成

$$x = 20 - t, \quad y = -20 + 2t, \quad (t = 0, \pm 1, \pm 2, \cdots)$$

在本章开始所提出的伟大的革命导师马克思曾经解答过的题目中，由于 x 及 y 代表男人、女人的个数，所以必须使得 $x \geqslant 0$，$y \geqslant 0$. 由 $x = 20 - t \geqslant 0$ 而得 $t \leqslant 20$，由 $y = -20 + 2t \geqslant 0$ 而得 $t \geqslant 10$，故有

$$10 \leqslant t \leqslant 20. \tag{15}$$

又小孩的个数由（1）式是 $z = 30 - x - y = 30 - t$. 由 $x = 20 - t$，$y = 2t - 20$，$z = 30 - t$ 和（15）式就得到下面的十一组解.

$$\left.\begin{aligned}x&=10\\y&=0\\z&=20\end{aligned}\right\},\quad \left.\begin{aligned}x&=9\\y&=2\\z&=19\end{aligned}\right\},\quad \left.\begin{aligned}x&=8\\y&=4\\z&=18\end{aligned}\right\},\quad \left.\begin{aligned}x&=7\\y&=6\\z&=17\end{aligned}\right\},$$

$$\left.\begin{aligned}x&=6\\y&=8\\z&=16\end{aligned}\right\},\quad \left.\begin{aligned}x&=5\\y&=10\\z&=15\end{aligned}\right\},\quad \left.\begin{aligned}x&=4\\y&=12\\z&=14\end{aligned}\right\},\quad \left.\begin{aligned}x&=3\\y&=14\\z&=13\end{aligned}\right\},$$

$$\left.\begin{aligned}x&=2\\y&=16\\z&=12\end{aligned}\right\},\quad \left.\begin{aligned}x&=1\\y&=18\\z&=11\end{aligned}\right\},\quad \left.\begin{aligned}x&=0\\y&=20\\z&=10\end{aligned}\right\}.$$

例 5 第五世纪末，我国古代数学家张丘建在他编写的《算经》里提出一个不定方程问题——世界数学史上有名的“百鸡问题”：

鸡翁一，值钱五，鸡母一，值钱三，鸡雏三，值钱一. 百钱买百鸡. 问鸡翁母雏各几何？（译：每一个大公鸡价值是 5 个钱，每一个母鸡价值是 3 个钱，每三个小鸡价值是 1 个钱，现有 100 个钱想买 100 只鸡. 问大公鸡，母鸡和小鸡各应买几只？）

解 设用 x，y，z 分别代表鸡翁，鸡母，鸡雏的数目，就得到下面的方程

$$5x+3y+\frac{z}{3}=100, \tag{16}$$

$$x+y+z=100. \tag{17}$$

由(16)和(17)式我们有

$$15x+9y+z-x-y-z=14x+8y=200,$$

即

$$7x+4y=100. \tag{18}$$

我们要解决这个问题，就是要求出上述方程的非负整数解。先解

$$7s+4t=1, \tag{19}$$

由于 $7=4+3,\ 4=3+1$，而得

$$1=4-3=4-(7-4)=-7+4\times 2.$$

因此(19)式的一个整数解是 $s=-1,\ t=2$。令 $x=100s$，$y=100t$，则由(19)式有

$$7x+4y=100(7s+4t)=100.$$

故(18)式的一个整数解是 $x=-100,\ y=200$。由定理1知道(18)式的一切整数解可以表示成

$$x=-100-4t,\quad y=200+7t,$$
$$(t=0,\ \pm 1,\ \pm 2,\ \cdots). \tag{20}$$

由于 x 及 y 代表鸡翁，鸡母的个数，所以必须使得 $x\geqslant 0,\ y\geqslant 0$。由 $-100-4t\geqslant 0$ 而得 $4t\leqslant -100$，由 $200+7t\geqslant 0$ 而得 $7t\geqslant -200$，因此

$$-\frac{200}{7}\leqslant t\leqslant -25.$$

由于 t 是整数，故 $t=-28,\ -27,\ -26,\ -25$。鸡雏的个数由(17)式是

$$z=100-x-y=100-(-100-4t)-(200+7t)=-3t.$$

由(20)式，$t=-28,\ -27,\ -26,\ -25$ 和 $z=-3t$ 就得到

下面四组解答:

$$\left.\begin{aligned}x&=12\\y&=4\\z&=84\end{aligned}\right\},\quad\left.\begin{aligned}x&=8\\y&=11\\z&=81\end{aligned}\right\},\quad\left.\begin{aligned}x&=4\\y&=18\\z&=78\end{aligned}\right\},\quad\left.\begin{aligned}x&=0\\y&=25\\z&=75\end{aligned}\right\}.$$

§3. 勾 股 数

定义 1 如果正整数 x, y, z 能满足下列不定方程

$$x^2+y^2=z^2, \tag{21}$$

则它们叫作勾股数.

我国古代数学书《周髀算经》曾提到"勾广三,股修四,径隅五"这个三边都是正整数的直角三角形,因此已经知道了不定方程(21)的一组正整数解 3, 4, 5. 在公元 263 年时,我国数学家刘徽写了一本数学书,书名叫作《九章算术》,其中有

$$3^2+4^2=5^2, \tag{22}$$

$$5^2+12^2=13^2, \tag{23}$$

$$7^2+24^2=25^2, \tag{24}$$

$$8^2+15^2=17^2, \tag{25}$$

$$20^2+21^2=29^2, \tag{26}$$

由此看来,我国古代数学家已经研究出(21)式的很多组正整数解.

显然 $x=0, y=0, z=0$; $x=0, y=z$; $x=0, y=-z$; $y=0, x=z$; 和 $y=0, x=-z$ 都是(21)式的解;除此以外(21)式的每一组解都不包含零. 如果 x, y, z 是(21)式的一组解,当然 $-x, y, z$; $x, -y, z$; $x, y, -z$; $x, -y, -z$; $-x, -y, z$; $-x, y, -z$; $-x, -y, -z$ 也都是(21)式的整数解. 以下我们将只讨论(21)式的正整数解,那就是说,我们将只讨论勾股数.

如果(21)式有正整数解且满足 $(x, y)=d>1$, 由 $d^2|x^2$,

$d^2|y^2$ 而得 $d^2|(x^2+y^2)$. 由(21)式有 $d^2|z^2$, 故得 $d|z$. 此时可将(21)式的两边同时约去 d. 由于 $\left(\frac{x}{d}, \frac{y}{d}\right)=1$, 所以在(21)式中可假定 $(x, y)=1$.

如果(21)式有正整数解且满足 $(x, y)=1$, 由 $(x, y)=1$ 得到 x, y 不可能都是偶数. 现在我们来证明 x, y 不可能都是奇数. 如果 x, y 都是奇数, 则有 $x=2m+1$, $y=2n+1$, 其中 m, n 都是非负整数. 此时有

$$x^2+y^2=(2m+1)^2+(2n+1)^2=4(m^2+n^2+m+n)+2,$$

即得 $2|(x^2+y^2)$, 但 $4\nmid(x^2+y^2)$. 由(21)式有 $2|z^2$, 但 $4\nmid z^2$, 这和 z 是一个整数而发生矛盾, 故 x, y 不可能都是奇数. 因此如果(21)式有正整数解且满足 $(x, y)=1$, 则 x, y 中有一个是偶数, 而另外一个是奇数. 所以我们不妨假定 x 是偶数.

定理 2 不定方程(21)的适合条件

$$x>0, \quad y>0, \quad z>0, \quad (x, y)=1, \quad 2|x \tag{27}$$

的一切正整数解可以用下列公式表示出来:

$$x=2ab, \quad y=a^2-b^2, \quad z=a^2+b^2. \tag{28}$$

这里 a 和 b 都是正整数, 而 $a>b$, $(a, b)=1$, $2\nmid(a+b)$.

证 由于 a 和 b 都是正整数且 $a>b$, 所以由(28)式有 $x=2ab>0$, $y=a^2-b^2>0$, $z=a^2+b^2>0$, 即 x, y, z 满足(27)式中的条件 $x>0$, $y>0$, $z>0$, $2|x$. 由(28)式我们有

$$x^2+y^2=4a^2b^2+(a^2-b^2)^2=a^4+2a^2b^2+b^4=(a^2+b^2)^2=z^2,$$

所以(28)式是满足(21)式的正整数解. 现设 $(x, y)=d$, 则有 $d|x$, $d|y$, $d^2|x^2$, $d^2|y^2$, $d^2|(x^2+y^2)$, 因此由(21)式得到 $d^2|z^2$, 即 $d|z$. 设 $y=dl$, $z=dm$, 则由(28)式我们有

$$2a^2 = a^2 - b^2 + a^2 + b^2 = y + z = d(l + m),$$
$$2b^2 = a^2 + b^2 - (a^2 - b^2) = z - y = d(m - l).$$
所以有 $d|2a^2$ 和 $d|2b^2$，而得 $d|2(a^2, b^2)$. 由于在(28)式中有 $(a, b) = 1$，而得 $(a^2, b^2) = 1$. 由 $d|2(a^2, b^2)$ 和 $(a^2, b^2) = 1$，得到 $d|2$. 由于 $a - b = a + b - 2b$ 和在(28)式中有 $2\nmid(a + b)$，而得
$$2\nmid(a + b), \quad 2\nmid(a - b),$$
即 $2\nmid(a^2 - b^2)$，又由(28)式有 $2\nmid y$. 由于 $2\nmid y$，$d|2$ 和 $(x, y) = d$，而得 $d = 1$，即 $(x, y) = 1$. 所以(28)式满足(27)式的所有条件.

又当 x, y, z 是适合(27)式中所有条件的(21)式的任一组正整数解时，x, y, z 可用(28)式中的公式表示出来(证明见习题 9)，故本定理得证.

例 6 求下列不定方程
$$4x - 9y + 5z = 8 \tag{29}$$
的所有整数解.

解 令 t 是一个整数并有
$$4x - 9y = t, \tag{30}$$
由(29)和(30)式有
$$t + 5z = 8. \tag{31}$$
由 $x = -2t$，$y = -t$ 是(30)式的一组整数解，并由定理 1，得到 $x = -2t + 9u$，$y = -t + 4u$，$u = 0, \pm 1, \pm 2, \cdots$ 时是(30)式的一切整数解. 由定理 1 和 $t = 3$，$z = 1$ 是(31)式的一组整数解得到
$$t = 3 - 5v, \quad z = 1 + v \tag{32}$$
是(31)式的一切整数解，而 $v = 0, \pm 1, \pm 2, \cdots$.将 $t = 3 - 5v$ 代入 $x = -2t + 9u$，得到
$$x = -6 + 10v + 9u, \tag{33}$$

将 $t = 3 - 5v$ 代入 $y = -t + 4u$，得到

$$y = -3 + 5v + 4u. \tag{34}$$

由(32)到(34)式知道(29)式的所有整数解是

$$x = -6 + 10v + 9u,$$
$$y = -3 + 5v + 4u,$$
$$z = 1 + v.$$

这里 u 和 v 是任意的整数.

例 7 求不定方程 $xy = x^2 + 6$ 的所有整数解.

解 由 $xy = x^2 + 6$ 得到 $x(x-y) = -6$，所以有 $x \mid (-6)$. 当 $x = 1$ 时 $y = 7$，当 $x = -1$ 时 $y = -7$. 当 $x = 2$ 时 $y = 5$，当 $x = -2$ 时 $y = -5$. 当 $x = 3$ 时 $y = 5$，当 $x = -3$ 时 $y = -5$. 当 $x = 6$ 时 $y = 7$，当 $x = -6$ 时 $y = -7$. 故 $xy = x^2 + 6$ 的所有整数解是

$$\left.\begin{matrix} x = 1 \\ y = 7 \end{matrix}\right\},\quad \left.\begin{matrix} x = -1 \\ y = -7 \end{matrix}\right\},\quad \left.\begin{matrix} x = 2 \\ y = 5 \end{matrix}\right\},\quad \left.\begin{matrix} x = -2 \\ y = -5 \end{matrix}\right\},$$

$$\left.\begin{matrix} x = 3 \\ y = 5 \end{matrix}\right\},\quad \left.\begin{matrix} x = -3 \\ y = -5 \end{matrix}\right\},\quad \left.\begin{matrix} x = 6 \\ y = 7 \end{matrix}\right\},\quad \left.\begin{matrix} x = -6 \\ y = -7 \end{matrix}\right\}.$$

§4. 费尔马问题的介绍

在 1637 年，法国著名数学家费尔马提出了下列的猜测：当 n 是一个大于 2 的整数时，则

$$x^n + y^n = z^n \tag{35}$$

这个不定方程没有正整数解. 这个猜测一直到现在还没有被人们证明. 虽然是这样，但人们常把这个猜测叫作“费尔马大定理”(Fermat's last theorem). 如果 k 是一个正整数而(35)式对一个正整数 n 没有正整数解，则我们将证明

$$x^{kn} + y^{kn} = z^{kn} \tag{36}$$

这个不定方程也没有正整数解. 因为如果 x, y, z 是满足(36)

式的一组正整数解，则由(36)式有

$$(x^k)^n + (y^k)^n = (z^k)^n, \tag{37}$$

由于 x, y, z 和 k 都是正整数，所以 x^k, y^k 和 z^k 也都是正整数．由(37)式就知道，这和(35)式没有正整数解发生矛盾．设 n 是一个大于 2 的正整数，当 n 是奇数时，则由第一章引理 11 知道 n 一定能被一个奇素数除尽．当 n 是偶数时，则有 $n = 2m$，其中 m 是一个正整数．当 m 是奇数时，则由第一章引理 11 知道 m 一定能被一个奇素数除尽，而由 $n = 2m$ 知道 n 一定能被一个奇素数 m 除尽．当 m 是偶数时，则由 $n = 2m$ 知道 n 一定能被 4 除尽．所以如果我们能够证明(35)式对于 $n = 4$ 和 n 等于任何奇素数都没有正整数解，则"费尔马大定理"就一定成立．现在我们将证明(35)式对于 $n = 4$ 是没有正整数解的．

引理 3 不定方程

$$x^4 + y^4 = z^4 \tag{38}$$

没有正整数解．

证 我们只要能证明

$$x^4 + y^4 = u^2 \tag{39}$$

没有正整数解就行了．假设(39)式有正整数解，那么在满足(39)式的所有的各组正整数解当中，必有一组解中的 u 是最小的，即存在一个最小的正整数 u_1，使

$$x^4 + y^4 = u_1^2 \tag{40}$$

成立，而其中的 x 和 y 都是正整数．这时一定有 $(x, y) = 1$，不然的话，就有 $(x, y) = d > 1$．由 $d^4|x^4$, $d^4|y^4$ 和(40)式得到 $d^4|u_1^2$，即 $d^2|u_1$．将(40)式两边同时除以 d^4 就得到

$$\left(\frac{x}{d}\right)^4 + \left(\frac{y}{d}\right)^4 = \left(\frac{u_1}{d^2}\right)^2. \tag{41}$$

由于 $d > 1$，有 $0 < \frac{u_1}{d^2} < u_1$．(41)式和假设 u_1 是一个最小

的正整数使 (40) 式成立而发生矛盾，所以有 $(x, y)=1$. 由于 $(x, y)=1$ 知道 x, y 不能都是偶数. 现在我们将证明 x, y 不能都是奇数. 如果

$$x=2m+1, \quad y=2n+1,$$

则有 $x^4+y^4=(2m+1)^4+(2n+1)^4$, 得到 $2|(x^4+y^4)$, 但 $4\nmid(x^4+y^4)$. 由 (40) 式有 $2|u_1^2$, 但 $4\nmid u_1^2$, 这和假设 u_1 是正整数而发生矛盾. 所以 x, y 不能都是奇数. 设 x 是偶数, y 是奇数. 将 (40) 式改写成

$$(x^2)^2+(y^2)^2=u_1^2. \tag{42}$$

由 $(x^2, y^2)=1$, $2|x^2$, (42) 式和定理 2 有

$$x^2=2ab, \quad y^2=a^2-b^2, \quad u_1=a^2+b^2. \tag{43}$$

这里 a 和 b 都是正整数, 且 $a>b$, $(a, b)=1$, $2\nmid(a+b)$. 由 $2\nmid(a+b)$ 知道 a, b 不能都是偶数, a, b 也不可能都是奇数, 所以 a, b 二数中一个是偶数, 一个是奇数. 现在我们将证明 b 不是奇数. 先假定 b 是奇数, 设 $b=2m+1$. 由 y 是奇数设 $y=2n+1$, 得到 $b^2+y^2=(2m+1)^2+(2n+1)^2$, 所以有 $2|(b^2+y^2)$, 但 $4\nmid(b^2+y^2)$. 由 (43) 式有 $a^2=b^2+y^2$, 所以有 $2|a^2$, 但 $4\nmid a^2$, 这和假设 a 是一个正整数而发生矛盾. 所以肯定 b 是偶数而 a 是奇数. 设 $b=2b_1$, b_1 是一个正整数. 由 (43) 式有

$$\left(\frac{x}{2}\right)^2=ab_1. \tag{44}$$

因为 $(a, b)=1$, 所以 $(a, b_1)=1$. 由 (44) 式和 x 是偶数知道存在有适当的正整数 c, d, 能使

$$a=c^2, \quad b_1=d^2, \quad (c, d)=1. \tag{45}$$

因为 a 是奇数, 所以 $2\nmid c$. 因为 $b=2b_1$, 所以 $b=2d^2$. 由 (43) 和 (45) 式有 $y^2=a^2-b^2=(c^2)^2-(2d^2)^2$, 得到

$$(2d^2)^2+y^2=(c^2)^2. \tag{46}$$

因为 $(a, b) = 1$，所以 $(c^2, 2d^2) = 1$．而由(46)式有 $(2d^2, y) = 1$．由(46)式和定理 2 有

$$2d^2 = 2kl, \quad y = k^2 - l^2, \quad c^2 = k^2 + l^2. \tag{47}$$

这里 k 和 l 都是正整数，且 $(k, l) = 1$．由(47)式得到

$$d^2 = kl.$$

因为 $(k, l) = 1$，故得

$$k = K^2, \qquad l = L^2. \tag{48}$$

其中 K 和 L 都是正整数．由(47)和(48)式有

$$K^4 + L^4 = c^2. \tag{49}$$

由(45)式和 c 是一个正整数有 $c \leqslant c^2 = a \leqslant a^2$，故由(43)式得到 $c < u_1$．由(49)式，和 $0 < c < u_1$，这和假设 u_1 是一个满足(40)式的最小正整数发生矛盾，所以(39)式没有正整数解，因而(38)式也没有正整数解．

有很多数学家为了"费尔马大定理"绞尽了脑汁，但是到现在为止，我们还只知道当 $2 < n < 100000$ 时（当然还包括这些数的任何倍数，这结果可见于 Math. Notices, 1976 年第一期），(35)式没有正整数解．

习　　题

1. 判断下列方程式有无整数解：

(i) $x^3 + 3x^2 + 4x + 2 = 0$.

(ii) $x^9 + x^5 - x^4 - 2x^2 + 3x - 37 = 0$.

(iii) $x^7 + 3x^5 + 3x + 1005973 = 0$.

2. 求下列不定方程的整数解：

(i) $7x + 15y = 0$.

(ii) $9x - 11y = 1$.

(iii) $17x + 40y = 280$.

(iv) $133x - 105y = 217$.

(v) $49x - 56y + 14z = 35$.

3. 求下列不定方程的整数解:

(i) $14021x + 38057y = 426639$.

(ii) $20746x - 63581y = 323$.

4. 求
$$\begin{cases} 5x + 7y + 2z = 24 \\ 3x - y - 4z = 4 \end{cases}$$
的正整数解.

5. 取一分、二分、五分的硬币共十枚,付给一角八分钱,问有几种不同的取法?

6. 有布 7 丈 5 尺,裁剪成大人和小孩的衣料,大人一件衣服用布 7 尺 2 寸,小孩一件衣服用布 3 尺,问各裁剪多少件衣服恰好把布用尽?

7. 某个二位数是它的个位数和十位数乘积的 3 倍,问这二位数是多少?

8. 证明:如果 a 和 b 是二个互素的正整数,则一定存在二个整数 x, y 使得
$$ax + by = 1.$$

9. 证明不定方程
$$x^2 + y^2 = z^2$$
的适合条件 $(x, y) = 1$, $2|x$ 的一切正整数解可以表示成
$$x = 2ab, \quad y = a^2 - b^2, \quad z = a^2 + b^2.$$
这里 a 和 b 都是正整数,且 $a > b$, $(a, b) = 1$, $2\nmid(a + b)$.

10. 证明:边长为整数的直角三角形,当斜边与一直角边长之差为 1 时,它的三个边长可表示成:$2b + 1$, $2b^2 + 2b$, $2b^2 + 2b + 1$,其中 b 是任意正整数.

11. 证明:不定方程
$$x^4 - 4y^4 = z^2$$
没有正整数解.

第四章　一次同余式及解法

§1. 同余的概念

在日常生活中，我们所要注意的常常不是某些整数，而是这些整数用某一固定的正整数去除所得的余数．例如我们问现在是几点钟，就是用 24 去除某一个总的时数所得的余数．比如从北京开往广州的火车，20 点 55 分开，全程的时间是 34 小时 15 分．如果问什么时候到广州，则答案不是 55 点 10 分而是 7 点 10 分．又如问今天是星期几，就是问用 7 去除某一个总的天数所得的余数．比如 1978 年的元旦是星期日，请问 1979 年的元旦是星期几？因为 1978 年有 365 天，而 $365 = 7 \times 52 + 1$，所以 1979 年的元旦应是星期一．由于同是几点钟或同为星期几，常常在生活中有同样的意义，这样就在数学中产生了"同余"的概念．这个概念的产生可以说大大丰富了数学的内容．

定义 1　如果 a 和 b 都是整数而 m 是一个固定的正整数，则当 $m|(a-b)$（即 m 能够整除 $a-b$）时，我们就说 a，b 对模 m 同余，记作 $a \equiv b \pmod m$．当 m 不能够整除 $a-b$ 时，则我们就说 a，b 对模 m 不同余，记作 $a \not\equiv b \pmod m$．

例 1　我们有 $29 \equiv 2 \pmod 9$．

$$93 \equiv -7 \pmod{50}.$$

证　由于 $29-2=27=3\times 9$，所以有 $29 \equiv 2 \pmod 9$．由于 $93-(-7)=93+7=2\times 50$，所以有 $93 \equiv -7 \pmod{50}$．

例 2　我们有 $161 \not\equiv 0 \pmod 8$．

$$257 \not\equiv 16 \pmod{32}.$$

证 由于 $161-0=8\times 20+1$，而得 $8\nmid(161-0)$，所以有 $161\not\equiv 0 \pmod 8$. 由于 $257-16=241=32\times 7+17$，而得 $32\nmid(257-16)$，所以有 $257\not\equiv 16 \pmod{32}$.

引理 1 当 a 是整数而 m 是一个正整数时，则有

$$a\equiv a \pmod m.$$

证 由于 $a-a=m\times 0$，而得 $m\mid(a-a)$，所以有 $a\equiv a \pmod m$.

引理 2 如果 a，b 都是整数而 m 是一个正整数，则当

$$a\equiv b \pmod m$$

成立时，我们有

$$b\equiv a \pmod m.$$

证 由于 $a\equiv b \pmod m$，得到 $a-b=mt$，其中 t 是一个整数. 又有 $b-a=m(-t)$，由于 $-t$ 也是一个整数，而得 $m\mid(b-a)$，所以有 $b\equiv a \pmod m$.

引理 3 如果 a，b，c 都是整数而 m 是一个正整数，则当

$$a\equiv b \pmod m$$

$$b\equiv c \pmod m$$

都成立时，我们有

$$a\equiv c \pmod m.$$

证 由于 $a\equiv b \pmod m$，得到

$$a-b=mt, \tag{1}$$

其中 t 是一个整数，由 $b\equiv c \pmod m$，得到

$$b-c=ms, \tag{2}$$

其中 s 是一个整数，将 (1) 和 (2) 式相加得到

$$a-c=a-b+b-c=mt+ms=m(t+s).$$

由于 $t+s$ 也是一个整数，所以有

$$a\equiv c \pmod m.$$

引理 4 如果 a, b, c, d 都是整数，而 m 是一个正整数，则当

$$a \equiv b \pmod{m}$$
$$c \equiv d \pmod{m}$$

都成立时，我们有

$$a + c \equiv b + d \pmod{m},$$
$$a - c \equiv b - d \pmod{m}.$$

证 由于 $a \equiv b \pmod{m}$，得到

$$a - b = ms, \tag{3}$$

其中 s 是一个整数. 由于 $c \equiv d \pmod{m}$，得到

$$c - d = mt, \tag{4}$$

其中 t 是一个整数. 由 (3) 和 (4) 式得到

$$(a + c) - (b + d) = a - b + c - d = ms + mt$$
$$= m(s + t).$$

由于 $s + t$ 是一个整数，所以有 $a + c \equiv b + d \pmod{m}$. 由(3) 和 (4) 式得到

$$a - c - (b - d) = a - b - c + d = a - b - (c$$
$$- d) = m(s - t),$$

由于 $s - t$ 是一个整数，所以有 $a - c \equiv b - d \pmod{m}$.

引理 5 如果 a, b, c 都是整数，而 m 是一个正整数，则当

$$a \equiv b \pmod{m}$$

成立时，我们有

$$ac \equiv bc \pmod{m}.$$

证 由于 $a \equiv b \pmod{m}$，得到

$$a - b = ms, \tag{5}$$

其中 s 是一个整数，将 (5)式两边同时乘以 c，得到

$$ac - bc = (a - b)c = mcs.$$

由于 cs 是一个整数，所以有 $ac \equiv bc \pmod m$.

引理 6 如果 a, b, c, d 都是整数，而 m 是一个正整数，则当

$$a \equiv b \pmod m$$

$$c \equiv d \pmod m$$

都成立时，我们有

$$ac \equiv bd \pmod m.$$

证 由 $a \equiv b \pmod m$ 和引理 5，得到

$$ac \equiv bc \pmod m. \tag{6}$$

由 $c \equiv d \pmod m$ 和引理 5，得到

$$bc \equiv bd \pmod m. \tag{7}$$

由 (6), (7) 式和引理 3，我们有 $ac \equiv bd \pmod m$.

引理 7 如果 a, b 都是整数，而 m 和 n 都是正整数，则当

$$a \equiv b \pmod m$$

成立时，我们有

$$a^n \equiv b^n \pmod m.$$

证 当 $n = 1$ 时显见本引理成立. 现设 $n \geqslant 2$. 在引理 6 中取 $c = a, d = b$，由引理 6 我们有

$$a^2 \equiv b^2 \pmod m. \tag{8}$$

故当 $n = 2$ 时本引理成立. 现设 $n \geqslant 3$. 在引理 6 中取 $c = a^2, d = b^2$，则由 (8) 式和引理 6 我们有

$$a^3 \equiv b^3 \pmod m. \tag{9}$$

故当 $n = 3$ 时本引理成立. 如果 $n \geqslant 4$，则可由引理 6 和陆续使用这样的方法而得到 $a^n \equiv b^n \pmod m$.

引理 8 如果 $a_1, a_2, \cdots, a_n, b_1, b_2, \cdots, b_n$ 都是整数，而 m 和 n 都是正整数，则当

$$a_1 \equiv b_1 \pmod m$$

$$a_2 \equiv b_2 \pmod m$$

$$\cdots\cdots\cdots\cdots$$

$$a_n \equiv b_n \pmod m$$

都成立时，我们有

$$a_1 + a_2 + \cdots + a_n \equiv b_1 + b_2 + \cdots + b_n \pmod m.$$

证 由 $a_1 \equiv b_1 \pmod m$，$a_2 \equiv b_2 \pmod m$ 和引理 4，我们有

$$a_1 + a_2 \equiv b_1 + b_2 \pmod m. \tag{10}$$

故当 $n = 2$ 时本引理成立。现设 $n \geqslant 3$。由 $a_3 \equiv b_3 \pmod m$，(10) 式和引理 4，我们有

$$a_1 + a_2 + a_3 \equiv b_1 + b_2 + b_3 \pmod m. \tag{11}$$

故当 $n = 3$ 时本引理也成立．如果 $n \geqslant 4$，则可由引理 4 和陆续使用这样的方法而得到

$$a_1 + a_2 + \cdots + a_n \equiv b_1 + b_2 + \cdots + b_n \pmod m.$$

例 3 求证 5874192 能被 9 整除．

证

$$5874192 = 5 \times 10^6 + 8 \times 10^5 + 7 \times 10^4 + 4 \times 10^3 + 10^2 + 9 \times 10 + 2. \tag{12}$$

由于 $10 \equiv 1 \pmod 9$，使用引理 7 知道，对于任意一个正整数 n 都有

$$10^n \equiv 1 \pmod 9. \tag{13}$$

由 (12)，(13) 式和引理 8，我们有

$$5874192 \equiv 5 + 8 + 7 + 4 + 1 + 9 + 2 \pmod 9.$$

由于 $5 + 8 + 7 + 4 + 1 + 9 + 2 = 36$，能被 9 整除，所以 5874192 能被 9 整除．

例 4 求证 2221435693 不能被 9 整除．

证

$$2221435693 = 2 \times 10^9 + 2 \times 10^8 + 2 \times 10^7 + 10^6 + 4 \times 10^5 + 3 \times 10^4 + 5 \times 10^3 + 6 \times 10^2$$

$$+9\times10+3. \tag{14}$$

由(13)，(14)式和引理8，我们有

$$2221435693\equiv2+2+2+1+4+3+5+6+9+3 \pmod 9, \tag{15}$$

由于 $2+2+2+1+4+3+5+6+9+3=37$，不能被9整除，所以由(15)式知道2221435693不能被9整除.

引理9 按照通常方法，把一个正整数 a 写成十进位数的形式，即

$$a=a_n10^n+a_{n-1}10^{n-1}+\cdots+a_0,\quad 0\leqslant a_i<10. \tag{16}$$

当9能够整除 $a_n+a_{n-1}+\cdots+a_0$ 时，则我们有9能够整除 a. 而当9不能整除 $a_n+a_{n-1}+\cdots+a_0$ 时，则9不能整除 a.

证 由(13)式和引理8，我们有

$$a\equiv a_n+a_{n-1}+\cdots+a_0 \pmod 9. \tag{17}$$

当9能够整除 $a_n+a_{n-1}+\cdots+a_0$ 时，则由(17)式我们得到9能够整除 a. 而当9不能够整除 $a_n+a_{n-1}+\cdots+a_0$ 时，则由(17)式我们得到9不能够整除 a.

例5 证明9能够整除221145236415.

证 由引理9我们有

$$221145236415\equiv2+2+1+1+4+5+2+3+6+4+1+5 \pmod 9, \tag{18}$$

又有

$$2+2+1+1+4+5+2+3+6+4+1+5=36. \tag{19}$$

由(18)，(19)式和9能整除36，所以9能够整除221145236415.

§2. 弃 九 法

弃九法是一种验算正整数计算的结果的方法. 假设我们

使用普通乘法运算方法求出正整数 a, b 的乘积是 P, 并令

$$a = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_0, \tag{20}$$

其中 $0 \leqslant a_i < 10$.

$$b = b_m 10^m + b_{m-1}10^{m-1} + \cdots + b_0, \tag{21}$$

其中 $0 \leqslant b_j < 10$. 又我们有

$$ab = P, \tag{22}$$

而

$$P = c_l 10^l + c_{l-1}10^{l-1} + \cdots + c_0, \tag{23}$$

其中 $0 \leqslant c_k < 10$. 由(13)式和引理 8, 我们有

$$a \equiv a_n + a_{n-1} + \cdots + a_0 \pmod 9, \tag{24}$$

$$b \equiv b_m + b_{m-1} + \cdots + b_0 \pmod 9, \tag{25}$$

$$P \equiv c_l + c_{l-1} + \cdots + c_0 \pmod 9. \tag{26}$$

由(22), (24)到(26)式我们得到

$$(a_n + a_{n-1} + \cdots + a_0)(b_m + b_{m-1} + \cdots + b_0) \equiv c_l + c_{l-1} + \cdots + c_0 \pmod 9, \tag{27}$$

所以, 我们说: 如果

$$(a_n + a_{n-1} + \cdots + a_0)(b_m + b_{m-1} + \cdots + b_0) \not\equiv c_l + c_{l-1} + \cdots + c_0 \pmod 9,$$

那么所求得的乘积是错误的. 以上所说就是弃九法的原则. 在实际验算时, 如果 $a_n, a_{n-1}, \cdots, a_0, b_m, b_{m-1}, \cdots, b_0, c_l, c_{l-1}, \cdots, c_0$ 中有 9 出现, 还可以把9去掉(因 $9 \equiv 0 \pmod 9$). 我们看一个例子.

例 6 求证 $28997 \times 39459 \neq 1144192613$.

证 由于 $28997 \equiv 2 + 8 + 7 \equiv 8 \pmod 9$,

$$39459 \equiv 3 + 4 + 5 \equiv 3 \pmod 9,$$

$$1144192613 \equiv 1 + 1 + 4 + 4 + 1 + 2 + 6 + 1 + 3 \equiv 5 \pmod 9,$$

但 $8 \times 3 = 24$, 而 $24 \not\equiv 5 \pmod 9$, 故得

$$28997 \times 39459 \neq 1144192613.$$

弃九法的优点在于验算时可以进行得比较快，但是应该特别注意当使用弃九法时，得出的结果虽然是

$$(a_n + a_{n-1} + \cdots + a_0)(b_m + b_{m-1} + \cdots + b_0)$$
$$\equiv c_l + c_{l-1} + \cdots + c_0 \pmod 9,$$

也还不能完全肯定原计算是正确的. 例如 $28997 \times 39459 = 1144192623$，如果有人计算出来的结果是 1144192533，那么用弃九法，就得

$$24 \equiv 6 \pmod 9,$$

而并未检查出错误来，因此这个验算方法是有它的缺点. 但是一般说来，如果我们对于二个正整数使用普通乘法运算方法来求乘积，然后再使用弃九法来检查而没有发现错误，则乘法运算所得的结果有较大的可能性是正确的.

例 7 求证 $12345 \times 67891 \neq 838114385$.

证 由于 $12345 \equiv 1 + 2 + 3 + 4 + 5 \equiv 6 \pmod 9$,

$$67891 \equiv 6 + 7 + 8 + 1 \equiv 4 \pmod 9,$$
$$838114385 \equiv 8 + 3 + 8 + 1 + 1 + 4 + 3 + 8 + 5 \equiv 5 \pmod 9,$$

但 $4 \times 6 = 24$，而 $24 \not\equiv 5 \pmod 9$，故得

$$12345 \times 67891 \neq 838114385.$$

§3. 一次同余式及解法

定义 2 如果 a, b 都是整数，而 m 是一个正整数，当 $a \not\equiv 0 \pmod m$ 时，我们把

$$ax + b \equiv 0 \pmod m \tag{28}$$

叫做模 m 的一次同余式.

引理 10 如果 c 是使 (28) 式成立的一个整数，即 $ac + b \equiv 0 \pmod m$，则满足 $x \equiv c \pmod m$ 的一切整数 x 都能

够使(28)式成立.

证 由 $x\equiv c \pmod m$,得到 $m\mid(x-c)$,即 $x-c=mn$,其中 n 是一个整数.由 $x=mn+c$ 和 $ac+b\equiv 0 \pmod m$,得到

$$ax+b\equiv a(mn+c)+b\equiv ac+b\equiv 0 \pmod m.$$

定义 3 如果 c 是使 $ac+b\equiv 0 \pmod m$ 成立的一个整数,则 $x\equiv c \pmod m$ 叫做(28)式的一个解. 这就是说今后我们把适合(28)式对模 m 相互同余的一切整数叫做(28)式的一个解.

引理 11 当 a, m 的最大公因数 (a, m) 不能够整除 b(即 $(a,m)\nmid b$)时,则一次同余式

$$ax+b\equiv 0 \pmod m, \quad a\not\equiv 0 \pmod m$$

没有整数解.

证 设存在有一个整数 c,使得 $ac+b\equiv 0 \pmod m$,即 $m\mid(ac+b)$,故存在有一个整数 n 使得 $ac+b=mn$, 而得

$$ac-mn=b. \tag{29}$$

设 $(a, m)=l$, 则有 $a=ld$, $m=le$, 其中 d 和 e 都是整数. 将它们代进(29)式,得到

$$b=ac-mn=cld-len=l(cd-en). \tag{30}$$

由 $cd-en$ 是整数和(30)式,得到 $l\mid b$, 但这和题设 $(a, m)\nmid b$ 发生矛盾

引理 12 当 $(a, m)=1$ 时,则一次同余式

$$ax+b\equiv 0 \pmod m, \quad a\not\equiv 0 \pmod m$$

有整数解.

证 由第三章引理 2 知道存在有二个整数 x, y 使得

$$ax+my=-b$$

成立. 即 $m\mid(ax+b)$, 故得 $ax+b\equiv 0 \pmod m$.

我们知道适合(28)式的整数 x, 也就是适合不定方程

$$ax + my = -b \tag{31}$$

的解答中的 x 的值，故同余式(28)可以使用解不定方程(31)式的方法去求解．我国古代数学家在解同余式方面的工作中也有非常卓越的成就．

例 8 求 $2x \equiv 179 \pmod{562}$ 的整数解．

解 因为 $(2, 562) = 2$，$2 \nmid (-179)$，所以由引理 11 知道 $2x \equiv 179 \pmod{562}$ 没有整数解．

例 9 求 $256x \equiv 179 \pmod{337}$ 的整数解．

解 因为 $(256, 337) = 1$，所以由引理 12 知道 $256x \equiv 179 \pmod{337}$ 有整数解．由于 $337 = 256+81$，$256 = 81 \times 3 + 13$，$81 = 13 \times 6 + 3$，$13 = 4 \times 3 + 1$，得到 $1 = 13 - 4 \times 3 = 13 - 4 \times (81 - 13 \times 6) = 25 \times 13 - 4 \times 81 = 25 \times (256 - 81 \times 3) - 4 \times 81 = 25 \times 256 - 79 \times 81 = 25 \times 256 - 79 \times (337 - 256) = 104 \times 256 - 79 \times 337$．
所以有

$$104 \times 256 \equiv 1 \pmod{337}. \tag{32}$$

由 $256x \equiv 179 \pmod{337}$ 和引理 5，我们有

$$104 \times 256x \equiv 104 \times 179 \pmod{337}. \tag{33}$$

由于 $104 \times 179 = 55 \times 337 + 81$，得到

$$104 \times 179 \equiv 81 \pmod{337}. \tag{34}$$

由(32)式到(34)式得到 $x \equiv 81 \pmod{337}$．

引理 12 如果 $ad \equiv bd \pmod{md}$，则有 $a \equiv b \pmod{m}$．
(证明留给读者)

例 10 求 $1215x \equiv 560 \pmod{2755}$ 的整数解．

解 因为 $(1215, 2755) = 5$，$5 \mid 560$，故由原式得到

$$243x \equiv 112 \pmod{551}. \tag{35}$$

因为 $(243, 551) = 1$，所以由引理 12 知道 $243x \equiv 112 \pmod{551}$ 有整数解．由于

$$551 = 2 \times 243 + 65, \quad 243 = 65 \times 3 + 48,$$
$$65 = 48 + 17, \quad 48 = 17 \times 2 + 14, \quad 17 = 14 + 3, \quad 14 = 3 \times 4 + 2, \quad 3 = 2 + 1,$$

得到

$$\begin{aligned} 1 &= 3 - 2 = 3 - (14 - 3 \times 4) = 5 \times 3 - 14 \\ &= 5 \times (17 - 14) - 14 = 5 \times 17 - 6 \times 14 \\ &= 5 \times 17 - 6 \times (48 - 17 \times 2) = 17 \times 17 - 6 \times 48 = 17 \times (65 - 48) - 6 \times 48 \\ &= 17 \times 65 - 23 \times 48 = 17 \times 65 - 23 \times (243 - 65 \times 3) = -23 \times 243 + 86 \times 65 = -23 \times 243 + 86 \times (551 - 2 \times 243) = 86 \times 551 - 195 \times 243. \end{aligned}$$

所以有

$$-195 \times 243 \equiv 1 \pmod{551}. \tag{36}$$

由(35)式和引理5我们有

$$-195 \times 243x \equiv -195 \times 112 \pmod{551}. \tag{37}$$

由于 $-195 \times 112 = 200 - 551 \times 40$，得到

$$-195 \times 112 \equiv 200 \pmod{551}. \tag{38}$$

由(36)式到(38)式得到 $x \equiv 200 \pmod{551}$. 由于 $2755 = 551 \times 5$ 和 $200 + 551 = 751$, $200 + 551 \times 2 = 1302$, $200 + 551 \times 3 = 1853$, $200 + 551 \times 4 = 2404$，所以 $1215x \equiv 560 \pmod{2755}$ 的5个不同解是

$$x \equiv 200, 751, 1302, 1853, 2404 \pmod{2755}.$$

例 11 求 $1296x \equiv 1125 \pmod{1935}$ 的整数解.

解 因为 $(1296, 1935) = 9$, $9 \mid 1125$，故由原式得到

$$144x \equiv 125 \pmod{215}. \tag{39}$$

因为 $(144, 215) = 1$，所以由引理12知道 $144x \equiv 125 \pmod{215}$ 有整数解. 由于 $215 = 144 + 71$, $144 = 71 \times 2 + 2$.

$71 = 2 \times 35 + 1$，得到

$$1 = 71 - 2 \times 35 = 71 - (144 - 71 \times 2) \times 35$$
$$= -144 \times 35 + 71 \times 71 = -144 \times 35 + 71$$
$$\times (215 - 144) = -106 \times 144 + 71 \times 215.$$

所以有

$$-106 \times 144 \equiv 1 \pmod{215}. \tag{40}$$

由 (39) 式和引理 5，我们有

$$-106 \times 144x \equiv -106 \times 125 \pmod{215}. \tag{41}$$

由于 $-106 \times 125 = 80 - 215 \times 62$，得到

$$-125 \times 106 \equiv 80 \pmod{215}. \tag{42}$$

由(40)到(42)式得到 $x \equiv 80 \pmod{215}$. 由于 $1935 = 215 \times 9$ 和 $80 + 215 = 295$, $80 + 2 \times 215 = 510$, $80+3 \times 215 = 725$, $80 + 4 \times 215 = 940$, $80 + 5 \times 215 = 1155$, $80 + 6 \times 215 = 1370$, $80 + 7 \times 215 = 1585$, $80 + 8 \times 215 = 1800$，所以 $1296x \equiv 1125 \pmod{1935}$ 的 9 个不同解是

$$x \equiv 80, 295, 510, 725, 940, 1155, 1370, 1585,$$
$$1800 \pmod{1935}.$$

§4. 孙 子 定 理

上节讨论了含一个未知数的同余式的解法，本节要讨论如何解下面重要的同余式组

$$x \equiv b_1 \pmod{m_1}, \quad x \equiv b_2 \pmod{m_2}, \cdots,$$
$$x \equiv b_k \pmod{m_k}. \tag{43}$$

在我国古代的《孙子算经》(纪元前后)里已经提出了这种形式的问题，并且很好地解决了它. 《孙子算经》里所提出的问题之一如下：

"今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何?""答曰二十三"(译：有一堆东西不知道有

多少个，用三来除这堆东西的个数时所得到的余数是二，用五来除这堆东西的个数时所得到的余数是三，用七来除这堆东西的个数时所得到的余数是二，问这堆东西共有多少个？答案是二十三个.）

把这个问题的提法用同余式的式子来表达，它可以被写成下面的形式：

解同余式组（设 x 是所求物数）

$$x \equiv 2 \pmod 3,\quad x \equiv 3 \pmod 5,\quad x \equiv 2 \pmod 7. \tag{44}$$

关于解一般的同余式组

$$x \equiv a \pmod 3,\quad x \equiv b \pmod 5,\quad x \equiv c \pmod 7, \tag{45}$$

则有

$$x \equiv 70a + 21b + 15c \pmod{105}.$$

关于这个一般的解法，在明朝程大位的《算法统宗》(1593) 里有一首歌，就是：

三人同行七十稀，
五树梅花廿一枝，
七子团圆整半月，
除百零五便得知.

（译：三个人共同走路，其中有七十岁以上的老年人的可能性很少，五棵梅花树总共二十一枝，七个孩子当正月十五日时在家中团圆，把一百零五的某个倍数减去，就得到答案.）所以关于解同余式组的问题，在我国古代有极光辉的研究成果. 我国古代数学家孙子发明了下面的中外驰名的定理.

定理1 如果 $k \geqslant 2$，而

$$m_1, m_2, \cdots, m_k$$

是二二互素的 k 个正整数，也就是说，在这 k 个正整数中任意取出二个正整数来，则这二个正整数是互素的. 令

$$M = m_1 m_2 \cdots m_k = m_1 M_1 = m_2 M_2 = \cdots = m_k M_k,$$

则同时满足同余式组

$$x \equiv b_1 \pmod{m_1}, \quad x \equiv b_2 \pmod{m_2}, \cdots,$$
$$x \equiv b_k \pmod{m_k} \tag{43}$$

的正整数解是

$$x \equiv b_1 M_1' M_1 + b_2 M_2' M_2 + \cdots + b_k M_k' M_k \pmod{M}. \tag{46}$$

这里 M_i' 是满足同余式

$$M_i' M_i \equiv 1 \pmod{m_i}$$

的正整数解，$i = 1, 2, \cdots, k$.

证 因为 $m_1, m_2, \cdots, m_k$ 是二二互素的，所以当 $i \neq j$ 时，则有 $(m_i, m_j) = 1$. 由于 $M_i = \frac{M}{m_i}$，得到 $(M_i, m_i) = 1$，所以

$$(M_1, m_1) = (M_2, m_2) = \cdots = (M_k, m_k) = 1.$$

由 $(M_1, m_1) = 1$ 和第三章引理 1，我们知道存在有二个整数 M_1', n_1 使得 $M_1 M_1' + m_1 n_1 = 1$. 所以存在有一个 M_1' 使得

$$M_1' M_1 \equiv 1 \pmod{m_1}$$

成立. 用同样方法知道对于每一个 M_i，一定存在有一个正整数 M_i' 使得

$$M_i' M_i \equiv 1 \pmod{m_i}. \tag{47}$$

另一方面，当 $i \neq j$ 时，则由 $(m_i, m_j) = 1$ 和 $M_j = \frac{M}{m_j}$ 得到 $m_i | M_j$. 所以有

$$b_j M_j' M_j \equiv 0 \pmod{m_i}. \tag{48}$$

由 (47) 式和 (48) 式我们有

$$b_1 M_1' M_1 + b_2 M_2' M_2 + \cdots + b_k M_k' M_k \equiv b_i M_i' M_i$$
$$\equiv b_i \pmod{m_i}. \tag{49}$$

由 $m_1, m_2, \cdots, m_k$ 是二二互素的和 (49) 式，知道 (46) 式是满足 (43) 式的正整数解. 如果 y 也能同时满足 (43) 式，则

由于(46)式是满足(43)式的正整数解，则得

$$x \equiv y \pmod{m_1}, \quad x \equiv y \pmod{m_2}, \cdots,$$
$$x \equiv y \pmod{m_k},$$

也就是 $m_1 | (x-y)$, $m_2 | (x-y)$, $\cdots$, $m_k | (x-y)$. 因为 $m_1, m_2, \cdots, m_k$ 是二二互素的，所以有 $M | (x-y)$，也就是

$$x \equiv y \pmod{M}.$$

所以 $x \equiv b_1 M_1' M_1 + b_2 M_2' M_2 + \cdots + b_k M_k' M_k \pmod{M}$ 是满足(43)式的唯一正整数解. 因此定理 1 得证.

现在我们来证明(45)式的整数解是 $x \equiv 70a + 21b + 15c \pmod{105}$. 此时在定理 1 中取 $m_1 = 3$, $m_2 = 5$, $m_3 = 7$, $b_1 = a$, $b_2 = b$, $b_3 = c$, 则 $M = 3 \times 5 \times 7 = 105$, $M_1 = \frac{105}{3} = 35$, $M_2 = \frac{105}{5} = 21$, $M_3 = \frac{105}{7} = 15$. 设 M_1' 是一个正整数，它满足 $M_1'M_1 \equiv 1 \pmod{3}$，则有 $1 \equiv M_1'M_1 \equiv 35M_1' \equiv 2M_1' \pmod{3}$，所以得到 $M_1' = 2$. 设 M_2' 是一个正整数，它满足 $M_2'M_2 \equiv 1 \pmod{5}$，则有 $1 \equiv M_2'M_2 \equiv 21M_2' \equiv M_2' \pmod{5}$，所以得到 $M_2' = 1$. 设 M_3' 是一个正整数，它满足 $M_3'M_3 \equiv 1 \pmod{7}$，则有 $1 \equiv M_3'M_3 \equiv 15M_3' \equiv M_3' \pmod{7}$，所以得到 $M_3' = 1$. 由于 $b_1 = a$, $b_2 = b$, $b_3 = c$, $M_1'M_1 = 2 \times 35 = 70$, $M_2'M_2 = 1 \times 21 = 21$, $M_3'M_3 = 1 \times 15 = 15$ 和(46)式，就得到(45)式的正整数解是 $x \equiv 70a + 21b + 15c \pmod{105}$.

我国古代数学家杨辉在 1275 年写了一本书，书名叫做《续古摘奇算法》，下面的三个例题可见《续古摘奇算法》一书.

例 12 七数剩一，八数剩一，九数剩三，问本数.（译：求一个正整数 x，用 7 来除 x 则余数是 1，用 8 来除 x 则余数是 1，用 9 来除 x 则余数是 3.）

解 依题意有

$x \equiv 1 \pmod 7$, $x \equiv 1 \pmod 8$, $x \equiv 3 \pmod 9$.
在定理 1 中取 $m_1 = 7$, $m_2 = 8$, $m_3 = 9$, $b_1 = b_2 = 1$, $b_3=3$,
此时有

$$M = 7 \times 8 \times 9 = 504,$$

$$M_1 = \frac{504}{7} = 72,$$

$$M_2 = \frac{504}{8} = 63,$$

$$M_3 = \frac{504}{9} = 56.$$

设 M_1' 是一个正整数，它满足 $M_1'M_1 \equiv 1 \pmod 7$，则有 $1 \equiv M_1'M_1 \equiv 72M_1' \equiv 2M_1' \pmod 7$，所以得到 $M_1'=4$. 设 M_2' 是一个正整数，它满足 $M_2'M_2 \equiv 1 \pmod 8$，则有 $1 \equiv M_2'M_2 \equiv 63M_2' \equiv 7M_2' \pmod 8$，所以 $M_2'=7$. 设 M_3' 是一个正整数，它满足 $M_3'M_3 \equiv 1 \pmod 9$，则有 $1 \equiv M_3'M_3 \equiv 56M_3' \equiv 2M_3' \pmod 9$，所以 $M_3' = 5$. 故由 (46) 式得到 $x \equiv 72 \times 4 + 7 \times 63 + 3 \times 5 \times 56 \equiv 57 \pmod{504}$，即

$$x = 57 + 504k, \quad k = 0, 1, 2, \cdots.$$

例 13 十一数余三，十二数余二，十三数余一，问本数。（译：求一个正整数 x，用 11 来除 x 则余数是 3，用 12 来除 x 则余数是 2，用 13 来除 x 则余数是 1.）

解 依题意有

$x \equiv 3 \pmod{11}$, $x \equiv 2 \pmod{12}$, $x \equiv 1 \pmod{13}$.
在定理 1 中取 $m_1 = 11$, $m_2 = 12$, $m_3 = 13$, $b_1 = 3$, $b_2 = 2$, $b_3 = 1$, 此时有

$$M = 11 \times 12 \times 13 = 1716,$$

$$M_1 = \frac{1716}{11} = 156,$$

$$M_2 = \frac{1716}{12} = 143,$$

$$M_3 = \frac{1716}{13} = 132.$$

设 M_1' 是一个正整数，它满足 $M_1'M_1 \equiv 1 \pmod{11}$，则有 $1 \equiv M_1'M_1 \equiv 156M_1' \equiv 2M_1' \pmod{11}$，故 $M_1' = 6$。设 M_2' 是一个正整数，它满足 $M_2'M_2 \equiv 1 \pmod{12}$，则有 $1 \equiv M_2'M_2 \equiv 143 M_2' \equiv 11M_2' \pmod{12}$，所以得到 $M_2' = 11$. 设 M_3' 是一个正整数，它满足 $M_3'M_3 \equiv 1 \pmod{13}$，则有 $1 \equiv M_3'M_3 \equiv 132M_3' \equiv 2M_3' \pmod{13}$，所以得到 $M_3' = 7$. 故由(46)式得到

$$x \equiv 3 \times 6 \times 156 + 2 \times 11 \times 143 + 7 \times 132$$
$$\equiv 14 \pmod{1716},$$ 即得

$$x = 14 + 1716k, \quad k = 0, 1, 2, \cdots.$$

例 14 二数余一，五数余二，七数余三，九数余四，问本数.（译：求一个正整数 x，用 2 来除 x 则余数是 1，用 5 来除 x，则余数是 2，用 7 来除 x 则余数是 3，用 9 来除 x 则余数是4。）

解 依题意有

$$x \equiv 1 \pmod{2}, \quad x \equiv 2 \pmod{5},$$
$$x \equiv 3 \pmod{7}, \quad x \equiv 4 \pmod{9}.$$

在定理 1 中取 $m_1 = 2$, $m_2 = 5$, $m_3 = 7$, $m_4 = 9$, $b_1 = 1$, $b_2 = 2$, $b_3 = 3$, $b_4 = 4$, 此时有

$$M = 2 \times 5 \times 7 \times 9 = 630,$$

$$M_1 = \frac{630}{2} = 315,$$

$$M_2 = \frac{630}{5} = 126,$$

$$M_3 = \frac{630}{7} = 90,$$

$$M_4 = \frac{630}{9} = 70.$$

设 M_1' 是一个正整数,它满足 $M_1'M_1 \equiv 1 \pmod{2}$, 则有 $1 \equiv M_1'M_1 \equiv 315M_1' \equiv M_1' \pmod{2}$,所以得到 $M_1'=1$. 设 M_2' 是一个正整数, 它满足 $M_2'M_2 \equiv 1 \pmod{5}$, 则有 $1 \equiv M_2'M_2 \equiv 126M_2' \equiv M_2' \pmod{5}$, 所以得到 $M_2' = 1$. 设 M_3' 是一个正整数, 它满足 $M_3'M_3 \equiv 1 \pmod{7}$, 则有 $1 \equiv M_3'M_3 \equiv 90M_3' \equiv 6M_3' \pmod{7}$, 所以得到 $M_3' = 6$. 设 M_4' 是一个正整数,它满足 $M_4'M_4 \equiv 1 \pmod{9}$, 则我们有 $1 \equiv M_4'M_4 \equiv 70M_4' \equiv 7M_4' \pmod{9}$, 所以得到 $M_4' = 4$. 故由(46)式得到

$$x \equiv 315 + 2 \times 126 + 3 \times 6 \times 90 + 4 \times 4 \times 70$$
$$\equiv 157 \pmod{630},$$

即得

$$x = 157 + 630k, \quad k = 0, 1, 2, \cdots.$$

例 16 韩信点兵: 有兵一队,若列成五行纵队,则末行一人,成六行纵队,则末行五人,成七行纵队,则末行四人,成十一行纵队,则末行十人,求兵数.

解 设 x 是所求兵数,则依题意

$$x \equiv 1 \pmod{5}, \quad x \equiv 5 \pmod{6},$$
$$x \equiv 4 \pmod{7}, \quad x \equiv 10 \pmod{11}.$$

在定理 1 中取 $m_1 = 5$, $m_2 = 6$, $m_3 = 7$, $m_4 = 11$, $b_1 = 1$, $b_2 = 5$, $b_3 = 4$, $b_4 = 10$, 此时有

$$M = 5 \times 6 \times 7 \times 11 = 2310,$$

$$M_1 = \frac{2310}{5} = 462,$$

$$M_2 = \frac{2310}{6} = 385,$$

$$M_3 = \frac{2310}{7} = 330,$$

$$M_4 = \frac{2310}{11} = 210.$$

设 M_1' 是一个正整数，它满足 $M_1'M_1 \equiv 1 \pmod 5$，则有 $1 \equiv M_1'M_1 \equiv 462 M_1' \equiv 2 M_1' \pmod 5$，所以得到 $M_1' = 3$. 设 M_2' 是一个正整数，它满足 $M_2'M_2 \equiv 1 \pmod 6$，则有 $1 \equiv M_2'M_2 \equiv 385 M_2' \equiv M_2' \pmod 6$，所以得到 $M_2' = 1$. 设 M_3' 是一个正整数，它满足 $M_3'M_3 \equiv 1 \pmod 7$，则有 $1 \equiv M_3'M_3 \equiv 330 M_3' \equiv M_3' \pmod 7$，所以得到 $M_3' = 1$. 设 M_4' 是一个正整数，它满足 $M_4'M_4 \equiv 1 \pmod{11}$，则有 $1 \equiv M_4'M_4 \equiv 210 M_4' \equiv M_4' \pmod{11}$. 故由 (46) 式得到

$$\begin{aligned} x &\equiv 3 \times 462 + 5 \times 385 + 4 \times 330 + 10 \times 210 \\ &\equiv 6731 \equiv 2111 \pmod{2310}, \end{aligned}$$

即得

$$x = 2111 + 2310k, \quad k = 0, 1, 2, \cdots.$$

习　　题

1. 1978 年的"八一"是星期二，1978 年 8 月份有 31 天，而 9 月份有 30 天，问 1978 年国庆是星期几？

2. 用弃九验算法检验下列计算是否正确：

(i) $4568 \times 7391 = 30746529$.

(ii) $2368 \times 846 = 2003328$.

(iii) $16 \times 937 \times 1559 = 23373528$.

(iv) $17^4 = 83521$.

(v) $23372428 \div 6236 = 3748$.

3. 证明：一次同余式

$$ax + b \equiv 0 \pmod m, \quad a \not\equiv 0 \pmod m$$

当 $(a, m) | b$ 时有解，并且解的个数是 $d = (a, m)$.

4. 解下列同余式：

(i) $258x \equiv 131 \pmod{348}$.

(ii) $3x \equiv 10 \pmod{29}$.

(iii) $47x \equiv 89 \pmod{111}$.

(iv) $660x \equiv 595 \pmod{1385}$.

5. 解下列同余式组:

(i) $\begin{cases} x \equiv 3 \pmod{7}, \\ x \equiv 5 \pmod{11}. \end{cases}$

(ii) $\begin{cases} x \equiv 2 \pmod{11}, \\ x \equiv 5 \pmod{7}, \\ x \equiv 4 \pmod{5}. \end{cases}$

(iii) $\begin{cases} x \equiv 1 \pmod{7}, \\ 3x \equiv 4 \pmod{5}, \\ 8x \equiv 4 \pmod{9}. \end{cases}$

6. 解下列各题:(杨辉:《续古摘奇算法》(1275))

(i) 七数剩一,八数剩二,九数剩四,问本数.

(ii) 二数余一,五数余二,七数余三,九数余五,问本数.

(iii) 十一数余三,七十二数余二,十三数余一,问本数.

7. 证明:同余式组

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv a \pmod{m_2} \end{cases}$$

的全部解是

$$x \equiv a \pmod{\{m_1, m_2\}}.$$

8. 证明:

(i) 若 $(m_1, m_2) = d$,则当 $d \mid (b_1 - b_2)$ 时,同余式组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases}$$

必定有解,它的全部解是

$$x \equiv x_0 \pmod{\{m_1, m_2\}}.$$

这里 x_0 是满足此同余式组的一个整数.

(ii) 若 $n_i \mid m_i$ $i = 1, 2, \cdots, k$.其中 $n_1, n_2, \cdots, n_k$ 两两

互素，且

$$\{n_1, n_2, \cdots, n_k\} = \{m_1, m_2, \cdots, m_k\},$$

则同余式组

$$x \equiv b_i \pmod{m_i}, \quad i = 1, 2, \cdots, k$$

在有解的情况下，它的解与同余式组

$$x \equiv b_i \pmod{n_i} \quad i = 1, 2, \cdots, k$$

的解相同.

9. 试解：

(i) $$\begin{cases} x \equiv 2 \pmod{7}, \\ x \equiv 5 \pmod{9}, \\ x \equiv 11 \pmod{15}. \end{cases}$$

(ii) 今有数不知总，以五累减之无剩，以七百一十五累减之剩十，以二百四十七累减之剩一百四十，以三百九十一累减之剩二百四十五，以一百八十七累减之剩一百零九，问总数若干？（黄宗宪：《求一术通解》，答数 10020.）

10. 甲，乙两港的距离不超过 5000 公里，今有三只轮船于某天零时同时从甲港开往乙港. 假定三只轮船每天 24 小时都是匀速航行，若干天后的零时第一只轮船首先到达，几天后的 18 时第二只轮船也到达，再过几天后的 8 时第三只轮船也到达了. 假若每天第一只轮船走 300 公里，第二只轮船走 240 公里，第三只轮船走 180 公里，问甲、乙两港实际距离是多少公里，三只轮船各走了多长时间？

习 题 解 答

第一章

1. 证：任意一个整数 a 都能够写成

$$a = 10n + b \tag{1}$$

的形式，其中 n 是一个整数而 $0 \leqslant b < 10$，由于 $2|10$，(1)式和假设 $2|b$，所以有 $2|a$，

2. 证：把 a 写成(1)的形式，则由于 $5|10$ 和假设 $5|b$，所以有 $5|a$。

3. 证：任意一个奇数 a 都能够写成

$$a = 4n + b \tag{2}$$

的形式，其中 n 是一个整数而 b 是奇数并且满足 $1 \leqslant b \leqslant 3$。又有

$$b^2 - 1 = \begin{cases} 0, & \text{当 } b = 1. \\ 8, & \text{当 } b = 3. \end{cases} \tag{3}$$

由(2)式可得到 $a^2 - 1 = (4n + b)^2 - 1$

$= 16n^2 + 8nb + b^2 - 1$

$$= 8(2n^2 + nb) + (b^2 - 1). \tag{4}$$

上式右端第一项是 8 的倍数，又由(3)式可知当 $b = 1$ 或 $b = 3$ 时有$8|(b^2 - 1)$。所以由(4)式得到$8|(a^2 - 1)$。另一种证明是，任意一个奇数 a 都能写成 $a = 2n + 1$ 的形式，其中 n 是整数。又有 $a^2 - 1 = 4n^2 + 4n = 4n(n+1)$。由于在 n 和 $n+1$ 中必有一个为偶数，所以 $n(n+1)$为偶数，即 $n(n+1) = 2m$，其中 m 为一个整数，故得 $a^2 - 1 = 8m$，所以 $8|(a^2 - 1)$。

4. 证：我们以 a，$a + 1$，$a + 2$，$a + 3$ 代表四个连续整数，其中 a 是一个整数，则 $a(a + 1)(a + 2)(a + 3) = (a^2+$

$3a)(a^2+3a+2)=[(a^2+3a+1)-1][(a^2+3a+1)+1]=(a^2+3a+1)^2-1.$

所以

$$a(a+1)(a+2)(a+3)+1=(a^2+3a+1)^2,$$

上式右端括弧内 a^2+3a+1 是一个整数，故 $(a^2+3a+1)^2$ 是一个平方数，

5. 证：a 和 $a-1$ 是二个连续整数，二个连续整数中必定有一个是偶数，所以

$$2|a(a-1)(2a-1). \qquad (5)$$

又任意整数 a 可以写成

$$a=3n+b \qquad (6)$$

的形式，其中 n 和 b 是整数，且 $1\leqslant b\leqslant 3$.

当 $b=1$ 时，$a-1=3n$，所以 $3|(a-1)$；

当 $b=2$ 时，$2a-1=6n+3$，所以 $3|(2a-1)$；

当 $b=3$ 时，$a=3n+3$，所以 $3|a$.

所以不论 b 是多少均有

$$3|a(a-1)(2a-1). \qquad (7)$$

由 (5) 式、(7) 式和 $(2,3)=1$ 就得到

$$6|a(a-1)(2a-1).$$

6. 证：由于 $a(a^2-1)=(a-1)\cdot a\cdot(a+1)$ 是三个连续整数的乘积，又由于三个连续整数中必定有一个是 3 的倍数，所以三个连续整数的乘积是 3 的倍数，故

$$3|a(a^2-1). \qquad (8)$$

又由第 3 题知道 $8|(a^2-1)$. 所以

$$8|a(a^2-1). \qquad (9)$$

由 (8) 式、(9) 式和 $(3,8)=1$ 可知

$$24|a(a^2-1).$$

7. 证：任意一个整数 a 能够写成

$$a = 12n + b$$

的形式，其中 n 是一个整数，而 $1 \leqslant b \leqslant 12$. 假若 $2 \nmid a$, $3 \nmid a$，则由于 $2 \mid 12n$, $3 \mid 12n$，所以 $2 \nmid b$, $3 \nmid b$. 因此 b 只能取 1, 5, 7, 11 四个值. 当 $b = 1, 5, 7$, 和 11 时，$a^2 + 23$ 分别是

$$(12n + 1)^2 + 23 = 144n^2 + 24n + 24,$$

$$(12n + 5)^2 + 23 = 144n^2 + 120n + 48,$$

$$(12n + 7)^2 + 23 = 144n^2 + 168n + 72,$$

$$(12n + 11)^2 + 23 = 144n^2 + 264n + 144.$$

上面四个式子的右端中的每一项都能被 24 整除，所以 a^2+23 能被 24 除尽.

注：此题也可以利用第 3 题和第 6 题的结果加以证明. 由于 $2 \nmid a$，所以 a 是奇数. 由第 3 题可知

$$8 \mid (a^2 - 1). \tag{10}$$

又由第 6 题可知

$$3 \mid a(a^2 - 1).$$

现 $3 \nmid a$，故由引理 13 得到

$$3 \mid (a^2 - 1). \tag{11}$$

由 (10) 式、(11) 式和 $(3, 8) = 1$ 而得到

$$24 \mid (a^2 - 1),$$

所以 $a^2 + 23 = (a^2 - 1) + 24$ 能被 24 整除.

8.

(i) 解：各数分解成素因数得

$$48 = 2 \times 2 \times 2 \times 2 \times 3 = 2^4 \times 3,$$

$$84 = 2 \times 2 \times 3 \times 7 = 2^2 \times 3 \times 7,$$

$$120 = 2 \times 2 \times 2 \times 3 \times 5 = 2^3 \times 3 \times 5.$$

所以 $(48, 84, 120) = 2^2 \times 3 = 12$.

(ii) 解：各数分解成素因数得

$$360 = 2^3 \times 3^2 \times 5,$$

$$810 = 2 \times 3^4 \times 5,$$
$$1260 = 2^2 \times 3^2 \times 5 \times 7,$$
$$3150 = 2 \times 3^2 \times 5^2 \times 7.$$

所以 $(360, 810, 1260, 3150) = 2 \times 3^2 \times 5 = 90.$

9

(i) 解：由于

	51425	13310	3
	39930	11495	
1	11495	1815	6
	10890	1815	
3	605	0	

所以 $(51425, 13310) = 605.$

(ii) 解：由于

1	353430	530145	
	353430	353430	
	0	176715	2

得到 $(353430, 530145) = 176715.$

又由于

	176715	165186	1
	165186	161406	
14	11529	3780	3
	11340	3780	
20	189	0	

得到 $(176715, 165186) = 189.$

所以 $(353430, 530145, 165186) = 189.$

(iii) 解：由于

	81719	52003	1
	52003	29716	
1	29716	22287	1
	22287	22287	
3	7429	0	

得到 $(81719, 52003) = 7429$.

由于

	33649	7429	4
	29716	3933	
1	3933	3496	1
	3496	3496	
8	437	0	

得到 $(33649, 7429) = 437$.

由于

	30107	437	68
	29716	391	
1	391	46	8
	368	46	
2	23	0	

得到 $(30107, 437) = 23$.

所以 $(81719, 52003, 33649, 30107) = 23$.

10.

(i) 解：由于

1	391	493	
	306	391	
1	85	102	3
	85	85	
	0	17	5

，

得到 $(391, 493) = 17$.

所以

$$\{391, 493\} = \frac{391 \times 493}{17} = 11339.$$

(ii) 解：由于

3	209	665	
	190	627	
2	19	38	5
		38	
	19	0	

，

得到 $(209, 665) = 19$.

所以

$$\{209, 665\} = \frac{209 \times 665}{19} = 7315.$$

又由于

	7315	4025	1
	4025	3290	
1	3290	735	4
	2940	700	
2	350	35	10
	350		
	0	35	

，

得到 $(7315, 4025) = 35$，因此

$$\{7315, 4025\} = \frac{7315 \times 4025}{35} = 841225.$$

所以 $\{209, 665, 4025\} = 841225$.

(iii) 解：由于

$$\begin{array}{r|r|r|l} & 1965 & 1834 & 1 \\ & 1834 & 1834 & \\ \cline{2-3} 14 & 131 & 0 & \end{array},$$

得到 $(1965, 1834) = 131$，因此

$$\{1965, 1834\} = \frac{1965 \times 1834}{131} = 27510.$$

由于

$$\begin{array}{r|r|r|l} 1 & 27510 & 30261 & \\ & 27510 & 27510 & \\ \cline{2-3} & 0 & 2751 & 10 \end{array},$$

得到 $(27510, 30261) = 2751$，因此

$$\{27510, 30261\} = \frac{27510 \times 30261}{2751} = 302610.$$

又由于

$$\begin{array}{r|r|r|l} & 302610 & 55020 & 5 \\ & 275100 & 55020 & \\ \cline{2-3} 2 & 27510 & 0 & \end{array},$$

得到 $(302610, 55020) = 27510$，因此

$$\{302610, 55020\} = \frac{302610 \times 55020}{27510} = 605220.$$

所以 $\{1965, 1834, 30261, 55020\} = 605220$.

11.

(i) 证：假设 $(a, b) = d$，则必然有

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1, \text{因此} \left(\left(\frac{a}{d}\right)^n, \left(\frac{b}{d}\right)^n\right) = 1. \text{ 即}$$

$$\left(\frac{a^n}{d^n}, \frac{b^n}{d^n}\right) = 1, \text{所以} (a^n, b^n) = d^n.$$

由于假设 $(a, b) = d$，因此得到

$$(a^n, b^n) = (a, b)^n.$$

(ii) 证：假设 $(a, b) = d$，那末 a 和 b 可以写成 $a = a_1 d$，$b = b_1 d$，并且 $(a_1, b_1) = 1$，因此

$$(na, nb) = (na_1 d, nb_1 d) = nd.$$

所以由假设得到 $(na, nb) = n(a, b)$.

12.

(i) 解：上一题关于最大公因数的性质显然可以推广到多于二个数的情形，所以

$$(216, 64, 1000) = (6^3, 4^3, 10^3)$$
$$= (6, 4, 10)^3 = 2^3 = 8.$$

(ii) 解：$(24000, 36000, 144000)$

$$= 1000 \times (24, 36, 144)$$
$$= 1000 \times 12 \times (2, 3, 12)$$
$$= 1000 \times 12 = 12000.$$

13. 证：因为 γ_i 是 α_i 和 β_i 两个数中小的那一个数，所以 $\dfrac{p_i^{\alpha_i}}{p_i^{\gamma_i}}$ 和 $\dfrac{p_i^{\beta_i}}{p_i^{\gamma_i}}$ 中必有一个数是 1，而另一个是整数，所以 $\left(\dfrac{p_i^{\alpha_i}}{p_i^{\gamma_i}}, \dfrac{p_i^{\beta_i}}{p_i^{\gamma_i}}\right) = 1$. 令 $i = 1, 2, \cdots, k$，就得到下面 k 个等式

$$\left(\frac{p_1^{\alpha_1}}{p_1^{\gamma_1}}, \frac{p_1^{\beta_1}}{p_1^{\gamma_1}}\right) = 1,$$

$$\left(\frac{p_2^{\alpha_2}}{p_2^{\gamma_2}}, \frac{p_2^{\beta_2}}{p_2^{\gamma_2}}\right) = 1,$$

$$\cdots\cdots\cdots\cdots$$

$$\left(\frac{p_k^{\alpha_k}}{p_k^{\gamma_k}}, \frac{p_k^{\beta_k}}{p_k^{\gamma_k}}\right) = 1.$$

由于 $p_1, p_2, \cdots, p_k$ 为不同的素数,所以由上面的等式得到

$$\left(\frac{p_1^{\alpha_1}}{p_1^{\gamma_1}} \frac{p_2^{\alpha_2}}{p_2^{\gamma_2}} \cdots \frac{p_k^{\alpha_k}}{p_k^{\gamma_k}}, \frac{p_1^{\beta_1}}{p_1^{\gamma_1}} \frac{p_2^{\beta_2}}{p_2^{\gamma_2}} \cdots \frac{p_k^{\beta_k}}{p_k^{\gamma_k}}\right) = 1,$$

即

$$\left(\frac{a}{p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}}, \frac{b}{p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}}\right) = 1.$$

所以

$$(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}.$$

又由 γ_i 和 δ_i 的定义可知 $\gamma_i + \delta_i = \alpha_i + \beta_i$, 即

$$\delta_i = (\alpha_i + \beta_i) - \gamma_i, \quad 1 \leqslant i \leqslant k.$$

由引理 10 得到

$$\begin{aligned}
\{a, b\} &= \frac{a \cdot b}{(a, b)} \\
&= \frac{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \cdot p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}}{p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}} \\
&= p_1^{\alpha_1+\beta_1-\gamma_1} p_2^{\alpha_2+\beta_2-\gamma_2} \cdots p_k^{\alpha_k+\beta_k-\gamma_k} \\
&= p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}.
\end{aligned}$$

此题说明，两个正整数的公共素因数的较小次幂的乘积就是这两个正整数的最大公因数．两个正整数的所有素因数的较大次幂的乘积就是这两个正整数的最小公倍数，对于多于两个数的情形,这个结论同样适用．

14. 解：要用方砖恰好铺满整个屋子,所用方砖的最大边长就应该是屋子的长与宽的最大公因数． 为了去掉小数，我们用厘米作为长度单位，屋子的长为 525 厘米，宽 325 厘米．

由于

$$(525, 325) = 5 \times (105, 65)$$
$$= 5 \times 5 \times (21, 13) = 5 \times 5 = 25,$$

所以 $(525, 325) = 25$.

答：所用方砖的最大边长是 25 厘米.

15. 解：木块的边长显然是木料的长、宽、厚的最大公因数. 我们用分作为长度单位，由于

$$357 = 3 \times 7 \times 17,$$
$$105 = 3 \times 5 \times 7,$$
$$84 = 2^2 \times 3 \times 7,$$

所以 $(357, 105, 84) = 3 \times 7 = 21$.

答：木块的边长是 2 寸 1 分.

16. 解：由于各班的学生都要组织在锻炼小组内，而且各小组的人数相同，所以每组的人数必须是三个班学生人数的公因数，求小组的最多人数就是求三个班学生人数的最大公因数，由于

$$54 = 2 \times 3 \times 3 \times 3 = 2 \times 3^3,$$
$$48 = 2 \times 2 \times 2 \times 2 \times 3 = 2^4 \times 3,$$
$$72 = 2 \times 2 \times 2 \times 3 \times 3 = 2^3 \times 3^2,$$

所以 $(54, 48, 72) = 2 \times 3 = 6$. 又

$$\frac{54}{6} = 9, \quad \frac{48}{6} = 8, \quad \frac{72}{6} = 12.$$

答：锻炼小组人数最多为 6 人. 这时甲班有 9 个组，乙班有 8 个组，丙班有 12 个组.

17. 证：由于 201 斤和 183 斤都是整数颗手榴弹的重量，所以每颗手榴弹的重量必定是它们的公因数. 它们的最大公因数是

$$(201, 183) = 3 \times (67, 61) = 3.$$

由于 3 是素数，而 3 的因数只有 1 和 3，因此每颗手榴弹的重量必定是 3 斤.

18. 解：两个行星同时回到原来位置所需的时间必定是各行星绕太阳转一周时间的公倍数，现在要计算它们回到原来位置所需的最少时间，所以是求它们绕一周所需时间的最小公倍数. 由于

$$225 = 3^2 \times 5^2,$$
$$365 = 5 \times 73,$$

所以 $\{225, 365\} = 3^2 \times 5^2 \times 73 = 16425$.

答：两个行星同时回到原来位置至少需 16425 日.

19. 解：要使每种规格的棋盒都能铺满底面，包装箱底面的边长应为各种棋盒底面边长的公倍数，所以箱底最小的边长就是各棋盒底面边长的最小公倍数，我们用毫米作为长度单位，以便使各个边长都成整数. 用分解素因数的办法得到

$$210 = 2 \times 3 \times 5 \times 7,$$
$$120 = 2^3 \times 3 \times 5,$$
$$140 = 2^2 \times 5 \times 7,$$
$$105 = 3 \times 5 \times 7,$$

所以 $\{210, 120, 140, 105\} = 2^3 \times 3 \times 5 \times 7 = 840$.

答：箱底边长最少是 840 毫米，即 84 厘米.

20. 解：由于队形要成为长方形，因此人数必须是行数的倍数，求最少的人数实际上就是求各行数的最小公倍数，用分解素因数的方法得

$$10 = 2 \times 5, \qquad 15 = 3 \times 5,$$
$$18 = 2 \times 3^2, \qquad 24 = 2^3 \times 3,$$

所以 $\{10, 15, 18, 24\} = 2^3 \times 3^2 \times 5 = 360$.

答：最少需要 360 人.

21. 解：同时啮合的各齿到下次再同时啮合时，其间各齿

轮都转过了整数圈，因此转过的齿数是各齿轮齿数的最小公倍数，由于

$$84 = 2^2 \times 3 \times 7,$$
$$36 = 2^2 \times 3^2,$$
$$60 = 2^2 \times 3 \times 5,$$
$$48 = 2^4 \times 3,$$

所以 $\{84, 36, 60, 48\} = 2^4 \times 3^2 \times 5 \times 7 = 5040.$ 又

$$\frac{5040}{84} = 60, \quad \frac{5040}{36} = 140, \quad \frac{5040}{60} = 84, \quad \frac{5040}{48} = 105.$$

答：各齿轮转过的圈数是：甲轮 60 圈，乙轮 140 圈，丙轮 84 圈，丁轮 105 圈.

22.

(i) 解：

$$\begin{array}{r|l}
2 & 16500 \\ \hline
2 & 8250 \\ \hline
3 & 4125 \\ \hline
5 & 1375 \\ \hline
5 & 275 \\ \hline
5 & 55 \\ \hline
 & 11
\end{array}$$

所以 $16500 = 2^2 \times 3 \times 5^3 \times 11.$

(ii) 解：

$$\begin{array}{r|l}
2 & 1452990 \\ \hline
3 & 726495 \\ \hline
5 & 242165 \\ \hline
7 & 48433 \\ \hline
11 & 6919 \\ \hline
17 & 629 \\ \hline
 & 37
\end{array}$$

所以 $1452990=2\times3\times5\times7\times11\times17\times37$.

23. 证：我们用反证法，假定$\sqrt[n]{A}$是有理分数，即

$$\sqrt[n]{A}=\frac{p}{q},\quad q>1,\text{ 且 }(p,q)=1.$$

由此而推出矛盾. 将上式两边各自乘 n 次方就得到

$$A=\frac{p^n}{q^n}.$$

由于 $(p,q)=1$，所以 $(p^n,q^n)=1$，且 $q^n>1$，因此 $\frac{p^n}{q^n}$ 不是整数，而 A 是整数. 故 $A=\frac{p^n}{q^n}$ 不可能成立. 这个矛盾是由于假定 $\sqrt[n]{A}$ 是有理分数而引起的，所以 $\sqrt[n]{A}$ 不可能是有理分数.

24. 证：假设$\frac{p}{q}$是方程的根，$|p|$ 和 q 都是正整数，且 $(|p|,q)=1$. 按题意我们只需证明 $q=1$.

由于 $\frac{p}{q}$ 是方程的根，所以它满足方程式，把它代入方程得到

$$\frac{p^n}{q^n}+a_1\frac{p^{n-1}}{q^{n-1}}+\cdots+a_{n-1}\cdot\frac{p}{q}+a_n=0.$$

在等式的两边同乘以 q^n，得到

$$p^n+a_1p^{n-1}q+\cdots+a_{n-1}pq^{n-1}+a_nq^n=0.$$

移项并取出公因子

$$p^n=-q(a_1p^{n-1}+a_2p^{n-2}q+\cdots+a_{n-1}pq^{n-2}+a_nq^{n-1}).$$

上式右端括弧中由于 $p,q,a_1,\cdots,a_n$ 都是整数，所以整个括弧中的值也是整数. 假如以M表示它的值，则

$$p^n=-qM.$$

因此 q 是 p^n 的因数，即 $q|p^n$，于是 $q|p$. 但是 $(|p|,q)=1$，所以必有 $q=1$.

25. 证：我们分二步来证明这个问题.

第一步证明：形如 $4n-1$ 的数必定含有形如 $4n-1$ 的素因数，这是因为奇素数能够写成 $4n-1$ 或者 $4n+1$ 的形式，这里 n 是整数. 而由于

$$\begin{aligned}(4n_1+1)(4n_2+1) &= 16n_1n_2+4n_1+4n_2+1\\ &= 4(4n_1n_2+n_1+n_2)+1,\end{aligned}$$

所以形如 $4n+1$ 的数相乘的乘积仍然是形如 $4n+1$ 的数. 因此把形如 $4n-1$ 的数分解成素因数的乘积时，这些素因数不可能都是形如 $4n+1$ 的数，而必然有形如 $4n-1$ 的数.

第二步假设形如 $4n-1$ 的数中只包含有 k 个素数：p_1，p_2，$\cdots$，p_k. 令 $a=4(p_1p_2\cdots p_k)-1$，则 p_1，p_2，$\cdots$，p_k 都不是 a 的素因数. 因为假若其中某一个 p_i $(1\leqslant i\leqslant k)$ 是 a 的素因数，则由于 $4(p_1p_2\cdots p_k)-a=1$，等式左端每项都有因数 p_i，因此左端是 p_i 的倍数而右端为 1. 这是不可能的. 现在假如 a 是素数，则由于 a 本身是形如 $4n-1$ 的数，且 a 不等于 p_1，p_2，$\cdots$，p_k 中的任何一个，这就与假设形如 $4n-1$ 的素数只有 k 个相矛盾. 假如 a 不是素数，则由第一步的证明可知 a 必含有形如 $4n-1$ 的素因数. 而 p_1，p_2，$\cdots$，p_k 都不是 a 的素因数，这说明除 p_1，p_2，$\cdots$，p_k 外还有形如 $4n-1$ 的素数存在. 这也与假设形如 $4n-1$ 的素数只有 k 个相矛盾. 因而形如 $4n-1$ 的素数的个数无限.

26. 由引理 6 可以知道，判断 N 是不是素数，只要把所有不大于 $\sqrt{N}$ 的素数去试除 N，假如没有一个能除尽 N，那末 N 就是素数，根据这个道理可以找出不超过 N 的所有素数：我们把 N 以内的自然数（1 除外）按次序排列：2，3，4，5，$\cdots$，N. 第一个数 2 是素数，我们在这些数中把 2 留下，按次地划去 2 以后的所有 2 的倍数（如 4，6，8，$\cdots$）. 2 后面没有被划掉的是 3，它也是素数，把 3 留下，再顺次划去 3 以后的所

有 3 的倍数，其中有的数也可能在划掉 2 的倍数时已被划掉了．在 3 后面没有被划去的是 5，可见 5 不是 2 或 3 的倍数（不然已被划去了），所以 5 也是素数．同样把 5 留下，顺次划去所有 5 的倍数．这样继续下去直到把所有不大于 $\sqrt{N}$ 的素数的倍数都划去，留下的就是不大于 N 的所有素数了．造 100 以内的素数表时，由于不大于 $\sqrt{100}$ 的素数只有 2，3，5 和 7．因此只要划去这四个素数的所有倍数，留下的数便是 100 以内的素数了．列表如下：

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

27.

(i) 解：由于

	435785667	131901878	3
	395705634	120240099	
3	40080033	11661779	3
	34985337	10189392	
2	5094696	1472387	3
	4417161	1355070	

2	677535	117317	5
	586585	90950	
1	90950	26367	3
	79101	23698	
2	11849	2669	4
	10676	2346	
2	1173	323	3
	969	204	
1	204	119	1
	119	85	
1	85	34	2
	68	34	
2	17	0	

，

所以 $(435785667, 131901878) = 17$.

(ii) 解：由于 $15959989 = 3989 \times 4001$,

右端的二个数 3989 和 4001 都是素数，它们显然都不是 7738 的因数，所以 $(15959989, 7738) = 1$.

28. (i) 解：因为

3	174530187
3	58176729
3	19392243
13	6464081
13	497237
23	38249
	1663,

所以 $174530187 = 3^3 \times 13^2 \times 23 \times 1663$.

(ii) 解：因为

$$
\begin{array}{r|l}
2 & 710352035484 \\ \hline
2 & 355176017742 \\ \hline
3 & 177588008871 \\ \hline
7 & 59196002957 \\ \hline
7 & 8456571851 \\ \hline
7 & 1208081693 \\ \hline
13 & 172583099 \\ \hline
17 & 13275623 \\ \hline
19 & 780919 \\ \hline
23 & 41101 \\ \hline
 & 1787
\end{array},
$$

所以

$$710352035484 = 2^2 \times 3 \times 7^3 \times 13 \times 17 \times 19 \times 23 \times 1787.$$

(iii) 解：因为

$$
\begin{array}{r|l}
2 & 40528613317500 \\ \hline
2 & 20264306658750 \\ \hline
3 & 10132153329375 \\ \hline
3 & 3377384443125 \\ \hline
3 & 1125794814375 \\ \hline
5 & 375264938125 \\ \hline
5 & 75052987625 \\ \hline
5 & 15010597525 \\ \hline
5 & 3002119505 \\ \hline
7 & 600423901 \\ \hline
 & 85774843
\end{array}
$$

$$
\begin{array}{r|l}
7 & 85774843 \\ \hline
7 & 12253549 \\ \hline
11 & 1750507 \\ \hline
11 & 159137 \\ \hline
17 & 14467 \\ \hline
23 & 851 \\ \hline
 & 37
\end{array},
$$

所以

$$
40528613317500 = 2^2 \times 3^3 \times 5^4 \times 7^3 \times 11^2 \times 17 \times 23 \times 37.
$$

29. 证：我们有 $F_5 = 2^{32} + 1 = 2^4 \times (2^7)^4 + 1 = (1 + 2^7 \times 5 - 1)(2^7)^4 + 1 = (1 + 2^7 \times 5)(2^7)^4 + 1 - (2^7)^4 = (1 + 2^7 \times 5)\{(2^7)^4 + (1 - 5 \times 2^7)(1 + 25 \times 2^{14})\} = 641 \times 6700417.$

第二章

1.

(i) 解：由表 1 的数值那一列知道不大于 420 的最大数是 256，又有 $2^8 = 256$. 由 $420 - 256 = 164$，再由表 1 的数值那一列知道不大于 164 的最大数是 128，又有 $2^7 = 128$. 由 $164 - 128 = 36$，再由表 1 的数值那一列知道不大于 36 的最大数是 32，又有 $2^5 = 32$. 由 $36 - 32 = 4$，再由表 1 的数值那一列知道不大于 4 的最大数是 4，又有 $2^2 = 4$. 由于

$$
\begin{aligned}
420 &= 256 + 128 + 32 + 4 \\
&= 1 \times 2^8 + 1 \times 2^7 + 0 \times 2^6 + 1 \times 2^5 \\
&\quad + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 0 \times 2 + 0,
\end{aligned}
$$

所以 $420 = (110100100)_2$.

(ii) 解：由表 1 的数值那一列知道不大于 2640 的最大

数是2048，又有 $2^{11}=2048$．由 $2640-2048=592$，再由表 1 的数值那一列知道不大于592的最大数是512，又有 $2^9=512$．由 $592-512=80$，再由表 1 的数值那一列知道不大于80的最大数是64，又有 $2^6=64$．由 $80-64=16$，再由表 1 的数值那一列知道不大于16的最大数是16，又有 $2^4=16$．由于

$$\begin{aligned}2640=2048+512+64+16=1\times 2^{11}\\ +0\times 2^{10}+1\times 2^9+0\times 2^8+0\times 2^7\\ +1\times 2^6+0\times 2^5+1\times 2^4+0\times 2^3\\ +0\times 2^2+0\times 2+0,\end{aligned}$$

所以 $2640=(101001010000)_2$。

2.

(i) 解：

$$\begin{aligned}(111111)_2=1\times 2^5+1\times 2^4+1\times 2^3+1\times 2^2\\ +1\times 2+1=63.\end{aligned}$$

(ii) 解：

$$\begin{aligned}(11100001)_2=1\times 2^7+1\times 2^6+1\times 2^5+0\times 2^4\\ +0\times 2^3+0\times 2^2+0\times 2+1=225.\end{aligned}$$

3.

(i) 解：由 $\frac{420}{8}=52+\frac{4}{8}$，得到 $b_0=4$。

由 $\frac{52}{8}=6+\frac{4}{8}$，得到 $b_1=4$，$b_2=6$，即 $420=(644)_8$。

(ii) 解：由 $\frac{2640}{8}=330$，得到 $b_0=0$。

由 $\frac{330}{8}=41+\frac{2}{8}$，得到 $b_1=2$．由 $\frac{41}{8}=5+\frac{1}{8}$，得到 $b_2=1$，$b_3=5$，即 $2640=(5120)_8$。

4.

(i) 解:

$$(256)_8 = 2 \times 8^2 + 5 \times 8 + 6 = 174.$$

(ii) 解:

$$(11300)_3 = 1 \times 8^4 + 1 \times 8^3 + 3 \times 8^2 + 0 \times 8 + 0 = 4800.$$

5.

(i) 解: 第一步先将这个二进制数依次分成三个数字为一组, $(101101101)_2 = (101\ \ 101\ \ 101)_2$, 然后使用 (2.2) 式中的式子 $(101)_2 = (5)_8$, 即得 $(101101101)_2 = (555)_8$.

(ii) 解: 第一步先将这个二进制数依次分成三个数字为一组, $(101011001101001)_2 = (101\ \ 011\ \ 001\ \ 101\ \ 001)_2$, 然后使用 (2.2) 式中的式子 $(101)_2 = (5)_8$, $(011)_2 = (3)_8$, $(001)_2 = (1)_8$, 即得

$$(101011001101001)_2 = (53151)_8.$$

6.

(i) 解: 使用 (2.2) 式中的式子 $(4)_8 = (100)_2$, $(0)_8 = (000)_2$, $(1)_8 = (001)_2$, 即得

$$(401)_8 = (100000001)_2.$$

(ii) 解: 使用(2.2)式中的式子有 $(1)_8 = (001)_2$, $(2)_3 = (010)_2$, $(7)_8 = (111)_2$, $(0)_8 = (000)_2$, 即得

$$(1270)_8 = (001010111000)_2 = (1010111000)_2.$$

7.

(i) 解: 由于

$$\begin{array}{r} (1\ 0\ 0\ 1)_2 \\ +\quad (1\ 0\ 1)_2 \\ \hline (1\ 1\ 1\ 0)_2 \end{array}, \qquad \begin{array}{r} (1\ 1\ 1\ 0)_2 \\ +\ (1\ 1\ 1\ 1)_2 \\ \hline (1\ 1\ 1\ 0\ 1)_2 \end{array}, \qquad \begin{array}{r} (1\ 1\ 1\ 0\ 1)_2 \\ +\quad (1\ 1\ 1)_2 \\ \hline (1\ 0\ 0\ 1\ 0\ 0)_2 \end{array},$$

因而有

$$(1001)_2 + (101)_2 + (1111)_2 + (111)_2 = (100100)_2.$$

(ii) 解：由于

$$
\begin{array}{r}
(1\,0\,1\,0\,1\,1)_2 \\
(1\,0\,0\,1\,1)_2 \\
\hline
(1\,1\,1\,1\,1\,0)_2
\end{array},
\qquad
\begin{array}{r}
(1\,1\,1\,1\,1\,0)_2 \\
(1\,1\,1\,1)_2 \\
\hline
(1\,0\,0\,1\,1\,0\,1)_2
\end{array},
$$

因而有

$$(101011)_2+(10011)_2+(1111)_2=(1001101)_2.$$

8.

(i) 解：由于

$$
\begin{array}{r}
(1\,1\,1)_2 \\
\times\ (1\,0\,1)_2 \\
\hline
(1\,1\,1)_2 \\
+\ (1\,1\,1\,0\,0)_2 \\
\hline
(1\,0\,0\,0\,1\,1)_2
\end{array},
$$

因而有 $(111)_2\times(101)_2=(100011)_2$.

(ii) 解：由于

$$
\begin{array}{r}
(1\,0\,0\,1)_2 \\
\times\quad (1\,1\,1)_2 \\
\hline
(1\,0\,0\,1)_2 \\
(1\,0\,0\,1\,0)_2 \\
+\ (1\,0\,0\,1\,0\,0)_2 \\
\hline
(1\,1\,1\,1\,1\,1)_2
\end{array},
\qquad
\begin{array}{r}
(1\,1\,1\,1\,1\,1)_2 \\
\times\qquad (1\,0\,1)_2 \\
\hline
(1\,1\,1\,1\,1\,1)_2 \\
+\ (1\,1\,1\,1\,1\,1\,0\,0)_2 \\
\hline
(1\,0\,0\,1\,1\,1\,0\,1\,1)_2
\end{array},
$$

因而有 $(1001)_2\times(111)_2\times(101)_2=(100111011)_2$.

9.

(i) 解：我们先采用惯用的减法运算，得到

$$
\begin{array}{r}
(1\,0\,1\,0\,1\,1\,1)_2 \\
-\quad (1\,1\,0\,0\,1)_2 \\
\hline
(1\,1\,1\,1\,1\,0)_2
\end{array},
\qquad
\begin{array}{r}
(1\,1\,1\,1\,1\,0)_2 \\
-\ \ (1\,1\,1\,1\,0)_2 \\
\hline
(1\,0\,0\,0\,0\,0)_2
\end{array},
$$

因而有 $(1010111)_2-(11001)_2-(11110)_2=(100000)_2$.

现在我们再使用求补数的方法来进行运算．先求

$(11001)_2$的补数而得到$(00111)_2=(111)_2$，然后将被减数$(1010111)_2$加上补数而得到

$$\begin{array}{r} (1\,0\,1\,0\,1\,1\,1)_2 \\ +\qquad\quad (1\,1\,1)_2 \\ \hline (1\,0\,1\,1\,1\,1\,0)_2 \end{array},$$

然后再减去$(100000)_2$，便获得$(1010111)_2-(11001)_2$的答案

$$\begin{array}{r} (1\,0\,1\,1\,1\,1\,0)_2 \\ -\quad (1\,0\,0\,0\,0\,0)_2 \\ \hline (1\,1\,1\,1\,1\,0)_2 \end{array}.$$

现在我们再来求$(111110)_2-(11110)_2$. 先求$(11110)_2$的补数而得到$(00010)_2=(10)_2$，然后将被减数$(111110)_2$加上补数而得到

$$\begin{array}{r} (1\,1\,1\,1\,1\,0)_2 \\ +\qquad\quad (1\,0)_2 \\ \hline (1\,0\,0\,0\,0\,0\,0)_2 \end{array}$$

然后再减去$(100000)_2$，便获得$(111110)_2-(11110)_2$的答案

$$\begin{array}{r} (1\,0\,0\,0\,0\,0\,0)_2 \\ -\quad (1\,0\,0\,0\,0\,0)_2 \\ \hline (1\,0\,0\,0\,0\,0)_2 \end{array},$$

因而有$(1010111)_2-(11001)_2-(11110)_2=(100000)_2$.

(ii) 解：我们先采用惯用的减法运算得到

$$\begin{array}{r} (1\,0\,1\,1\,0\,0\,0\,1)_2 \\ -\quad (1\,1\,0\,1\,1\,0\,0)_2 \\ \hline (1\,0\,0\,0\,1\,0\,1)_2 \end{array}, \qquad \begin{array}{r} (1\,0\,0\,0\,1\,0\,1)_2 \\ -\qquad (1\,1\,1\,1\,0)_2 \\ \hline (1\,0\,0\,1\,1\,1)_2 \end{array},$$

因而

$$(10110001)_2-(1101100)_2-(11110)_2=(100111)_2.$$

现在我们再使用求补数的方法来进行计算. 先求$(1101100)_2$的补数而得到$(0010100)_2=(10100)_2$，然后将被减数$(10110001)_2$加上补数$(10100)_2$而得到

$$\begin{array}{r} (10110001)_2 \\ +\quad (10100)_2 \\ \hline (11000101)_2 \end{array},$$

然后再减去$(10000000)_2$，便获得$(10110001)_2-(1101100)_2$的答案

$$\begin{array}{r} (11000101)_2 \\ -(10000000)_2 \\ \hline (1000101)_2 \end{array}.$$

现在我们再来求$(1000101)_2-(11110)_2$. 先求$(11110)_2$的补数而得到$(00010)_2=(10)_2$，然后将被减数$(1000101)_2$加上补数$(10)_2$而得到

$$\begin{array}{r} (1000101)_2 \\ +\quad (10)_2 \\ \hline (1000111)_2 \end{array},$$

然后再减去$(100000)_2$，便获得$(1000101)_2-(11110)_2$的答案

$$\begin{array}{r} (1000111)_2 \\ -\quad (100000)_2 \\ \hline (100111)_2 \end{array},$$

因而有

$$(10110001)_2-(1101100)_2-(11110)_2=(100111)_2.$$

10.

(i) 解：我们先采用惯用的除法运算得到

$$\begin{array}{r} (11)_2 \\ (100001)_2\overline{)\;(1100011)_2} \\ -(1000010)_2 \\ \hline (100001)_2 \\ -(100001)_2 \\ \hline (0)_2 \end{array},$$

因而有 $(1100011)_2 \div (100001)_2 = (11)_2$.

现在我们再使用求补数的方法来进行运算. 我们首先求除数 $(100001)_2$ 的补数而得到 $(011111)_2 = (11111)_2$, 然后将被除数 $(1100011)_2$ 加上补数 $(11111)_2$ 而得到

$$\begin{array}{r} (1100011)_2 \\ +\quad (11111)_2 \\ \hline (10000010)_2 \end{array},$$

然后再减去 $(1000000)_2$, 则得第一次减去除数后的余数, 即

$$\begin{array}{r} (10000010)_2 \\ -\quad (1000000)_2 \\ \hline (1000010)_2 \end{array}.$$

然后再将余数 $(1000010)_2$ 加上补数 $(11111)_2$ 再减去 $(1000000)_2$, 则得第二次减去除数后的余数, 即

$$\begin{array}{r} (1000010)_2 \\ +\quad (11111)_2 \\ \hline (1100001)_2 \\ -(1000000)_2 \\ \hline (100001)_2 \end{array}.$$

然后再将余数 $(100001)_2$ 加上补数 $(11111)_2$ 再减去 $(1000000)_2$, 则得第三次减去除数后的余数, 即

$$\begin{array}{r} (100001)_2 \\ +\quad (11111)_2 \\ \hline (1000000)_2 \\ -(1000000)_2 \\ \hline (0)_2 \end{array}.$$

不难看出, 因为总共减了三次刚好减完, 其商是 3, 将 3 变换成二进制数就是 $(11)_2$, 所以

$$(1100011)_2 \div (100001)_2 = (11)_2.$$

(ii) 解：我们先采用惯用的除法运算，得到

$$
\begin{array}{r}
(111)_2 \\
(111)_2 \overline{\big)\ (110001)_2} \\
-\ (11100)_2 \\
\hline
(10101)_2 \\
-\ (1110)_2 \\
\hline
(111)_2 \\
-\ (111)_2 \\
\hline
(0)_2
\end{array},
$$

因而有 $(110001)_2 \div (111)_2 = (111)_2$.

现在我们再使用求补数的方法来进行运算．首先求除数 $(111)_2$ 的补数而得 $(1)_2$．被除数减去除数(即加补数 $(1)_2$，再减去 $(1000)_2$)

$$
\left.\begin{array}{r}
(110001)_2 \\
+\quad (1)_2 \\
\hline
(110010)_2 \\
-\quad (1000)_2 \\
\hline
\end{array}\right\}\text{第一次减去除数，余数为}(101010)_2.
$$

$$
\left.\begin{array}{r}
(101010)_2 \\
+\quad (1)_2 \\
\hline
(101011)_2 \\
-\quad (1000)_2 \\
\hline
\end{array}\right\}\text{第二次减去除数，余数为}(100011)_2.
$$

$$
\left.\begin{array}{r}
(100011)_2 \\
+\quad (1)_2 \\
\hline
(100100)_2 \\
-\quad (1000)_2 \\
\hline
\end{array}\right\}\text{第三次减去除数，余数为}(11100)_2.
$$

$$
\left.\begin{array}{r}
(11100)_2 \\
+\quad (1)_2 \\
\hline
(11101)_2 \\
-\quad (1000)_2 \\
\hline
\end{array}\right\}\text{第四次减去除数，余数为}(10101)_2.
$$

$$
(10101)_2
$$

$$\left.\begin{array}{lr} & (1\,0\,1\,0\,1)_2 \\ + & (1)_2 \\ \hline & (1\,0\,1\,1\,0)_2 \\ - & (1\,0\,0\,0)_2 \\ \hline \end{array}\right\}\text{第五次减去除数，余数为}(1110)_2.$$

$$\left.\begin{array}{lr} & (1\,1\,1\,0)_2 \\ + & (1)_2 \\ \hline & (1\,1\,1\,1)_2 \\ - & (1\,0\,0\,0)_2 \\ \hline \end{array}\right\}\text{第六次减去除数，余数为}(111)_2.$$

$$\left.\begin{array}{lr} & (1\,1\,1)_2 \\ + & (1)_2 \\ \hline & (1\,0\,0\,0)_2 \\ - & (1\,0\,0\,0)_2 \\ \hline \end{array}\right\}\text{第七次减去除数，余数为}(0)_2.$$

$$(0)_2$$

不难看出，因为总共减了七次刚好减完，其商是 7，将 7 变换成二进制是 $(111)_2$，所以

$$(110001)_2 \div (111)_2 = (111)_2.$$

第三章

1.

(i) 解：方程式如果有整数解，它一定是常数项的因数。此方程的常数项 2 共有四个因数：1，−1，2 和 −2. 由于方程中每一项的系数都是正的，因此不可能有正数解，因为 x 取正值代入方程时，左端每一项都是正数. 所以方程的左端不可能为 0，因而只须将 −1 和 −2 代入方程验算. 验算结果只有 −1 满足方程式，因此方程具有唯一的整数解 $x=-1$.

(ii) 解：常数项的四个因数是：1，−1，37，和 −37，由于方程的第一项是 x 的九次方，它的方次数远大于其它各项的方次数. 并且各项的系数都不大. 所以 x 以绝对值较大的数代入时，方程第一项的绝对值远远大于其它各项绝对值的

和，因而方程的左端不可能为 0．例如以 $x=37$ 或 -37 代入时，方程的左端就不可能为 0（留给读者自己进行计算）．所以 37 和 -37 不是方程的解．又方程中除了常数项以外，其余各项的系数都很小，并且项数也不多，因此 x 以绝对值较小的数代入时，这些项的数值都很小．它们的绝对值的和小于常数项的绝对值时，方程的左端就不可能为 0．例如以 $x=1$ 或 -1 代入时，前面各项的绝对值的和远远小于常数项 37，所以 1 和 -1 也不是方程的解．因此原方程没有整数解．

对于某些方程，我们可以用类似上面讨论的办法来判断它的整数解，可以免去以常数项的因数代入验算的麻烦．

(iii) 解：由于

$$1005973=1009\times997,$$

而 1009 和 997 都是素数，所以常数项 1005973 有八个因数：±1，±997，±1009 和 ±1005973．

和 (ii) 中讨论的情况一样，这个方程的常数项非常大，其余各项系数不大，项数也不多．以 $x=\pm1$ 代入，这些项的绝对值远小于常数项，所以 ±1 不是方程的解．又这个方程最高次项为 x^7，而 x^5 和 x 项的系数不大，故以 $x=\pm1005973$ 代入时，第一项的绝对值远大于其余各项．同理由于 997 和 1009 接近于 1000，常数项 1005973 接近于 1000^2，故以 $x=\pm997$ 和 ±1009 代入时，首项的绝对值仍比其余各项大很多，因而 ±997，±1009，±1005973 都不是解（留给读者自己进行计算）．所以原方程无整数解．

2.

(i) 解：由于 $(7,15)=1$，且常数项是零，所以方程的整数解为：$x=-15t$，$y=7t$，$t=0,\pm1,\pm2,\cdots$．

(ii) 解：由于 $11=9+2$，$9=2\times4+1$，得到 $1=9-2\times4=9-4\times(11-9)=9\times5-11\times4$．所以 $x=5$，

$y=4$ 是方程的一组整数解．它的全部整数解是

$$x=5+11t,\quad y=4+9t,\quad t=0,\ \pm1,\ \pm2,\ \cdots.$$

(iii) 解：由于 $(17,40)=1$，所以方程有整数解．今先解 $17u+40v=1$．由于

$$40=2\times17+6,\quad 17=2\times6+5,\quad 6=5+1,$$

得到

$$1=6-5=6-(17-2\times6)=-17+3\times6$$
$$=-17+3\times(40-2\times17)=17\times(-7)$$
$$+40\times3.$$

因此 $u=-7$，$v=3$ 是 $17u+40v=1$ 的一组整数解．令 $x=280u$，$y=280v$，则

$$17x+40y=280(17u+40v)=280.$$

所以 $x=280\times(-7)=-1960$，$y=280\times3=840$ 是 $17x+40y=280$ 的一组整数解．它的全部整数解是 $x=-1960-40t$，$y=840+17t$，即

$$x=-40t,\quad y=7+17t,\quad t=0,\ \pm1,\ \pm2,\cdots.$$

(iv) 解：由于 $133=7\times19$，$105=7\times15$，$217=7\times31$，所以方程的解与

$$19x-15y=31$$

的解完全相同．今先解

$$19u-15v=1.$$

由于 $19=15+4$，$15=3\times4+3$，$4=3+1$，

而得 $1=4-3=4-(15-3\times4)=4\times4-15$

$$=4\times(19-15)-15=19\times4-15\times5.$$

所以 $u=4$，$v=5$ 是 $19u-15v=1$ 的一组整数解，因而 $x=31\times4=124$，$y=31\times5=155$ 是 $19x-15y=31$ 的一组整数解．它的全部整数解是

$$x=124+15t,\quad y=155+19t,$$

即

$$x = 4 + 15t,\quad y = 3 + 19t,\quad t = 0, \pm 1, \pm 2, \cdots.$$

(v) 解：由于 $49 = 7 \times 7$，$56 = 7 \times 8$，$14 = 7 \times 2$，和 $35 = 7 \times 5$，所以方程的解与

$$7x - 8y + 2z = 5$$

的解相同．令

$$7x - 8y = t,$$

则

$$t + 2z = 5.$$

易见 $x = 7t$，$y = 6t$ 是 $7x - 8y = t$ 的一组整数解．所以它的全部整数解是

$$\begin{cases} x = 7t + 8u, \\ y = 6t + 7u. \end{cases} \quad u = 0, \pm 1, \pm 2, \cdots.$$

而 $t = 1$，$z = 2$ 是 $t + 2z = 5$ 的一组整数解．它的全部整数解是

$$\begin{cases} t = 1 - 2v, \\ z = 2 + v. \end{cases} \quad v = 0, \pm 1, \pm 2, \cdots.$$

把 t 的表达式代到 x，y 的表达式中，得到原方程的全部整数解是

$$\begin{cases} x = 7 - 14v + 8u, \\ y = 6 - 12v + 7u, \\ z = 2 + v. \end{cases}$$

这里 u 和 v 通过一切整数．

3.

(i) 解：由于 $14021 = 7 \times 2003$，$38057 = 19 \times 2003$，$426639 = 213 \times 2003$，所以原方程的解与

$$7x + 19y = 213$$

的解完全相同．今先解

$$7u + 19v = 1.$$

由于

$$19=7\times 2+5,\quad 7=5+2,\quad 5=2\times 2+1,$$

得到

$$\begin{aligned}1&=5-2\times 2=5-2\times(7-5)=3\times 5-2\times 7\\&=3\times(19-7\times 2)-2\times 7\\&=7\times(-8)+19\times 3.\end{aligned}$$

所以 $u=-8$, $v=3$ 是 $7u+19v=1$ 的一组整数解. 因而

$$\begin{cases}x=(-8)\times 213=-1704\\y=3\times 213=639\end{cases}$$

是 $7x+19y=213$ 的一组整数解. 它的全部整数解是

$$\begin{cases}x=-1704-19t,\\y=639+7t.\end{cases}\quad t=0,\ \pm 1,\ \pm 2,\ \cdots.$$

即

$$\begin{cases}x=25-19t,\\y=2+7t.\end{cases}\quad t=0,\ \pm 1,\ \pm 2,\ \cdots.$$

(ii) 解: 因为 $(20746, 63581)=1$, 所以方程有解. 现先解方程

$$20746u-63581v=1.$$

由于

$$\begin{aligned}63581&=20746\times 3+1343,\\20746&=1343\times 15+601,\\1343&=601\times 2+141,\\601&=141\times 4+37,\\141&=37\times 3+30,\\37&=30\times 1+7,\\30&=7\times 4+2,\\7&=2\times 3+1,\end{aligned}$$

所以

$$
\begin{aligned}
1 &= 7 - 3 \times 2 = 7 - 3 \times (30 - 4 \times 7) \\
&= 13 \times 7 - 3 \times 30 = 13 \times (37 - 30) - 3 \times 30 \\
&= 13 \times 37 - 16 \times 30 \\
&= 13 \times 37 - 16 \times (141 - 3 \times 37) \\
&= 61 \times 37 - 16 \times 141 \\
&= 61 \times (601 - 4 \times 141) - 16 \times 141 \\
&= 61 \times 601 - 260 \times 141 \\
&= 61 \times 601 - 260 \times (1343 - 2 \times 601) \\
&= 581 \times 601 - 260 \times 1343 \\
&= 581 \times (20746 - 15 \times 1343) - 260 \times 1343 \\
&= 581 \times 20746 - 8975 \times 1343 \\
&= 581 \times 20746 - 8975 \times (63581 - 3 \times 20746) \\
&= 27506 \times 20746 - 8975 \times 63581.
\end{aligned}
$$

因此 $u = 27506$, $v = 8975$ 是方程

$$20746u - 63581v = 1$$

的解．因而

$$\begin{cases} x = 27506 \times 323 = 8884438 \\ y = 8975 \times 323 = 2898925 \end{cases}$$

是原方程的一组整数解．它的全部整数解是

$$\begin{cases} x = 8884438 + 63581t, \\ y = 2898925 + 20746t. \end{cases} \quad t = 0, \pm 1, \pm 2, \cdots.$$

这里 t 通过全部整数，因而 $t + k$ (k 是某固定整数)也通过全部整数．所以在上面的解中以 $t + k$ 代以 t 后仍为原方程的全部解．但这时适当的选择 k 可以使前面的常数变小一些．例如在上面的解中以 $t - 139$ 代以 t 就得到解为

$$\begin{cases} x = 46679 + 63581t, \\ y = 15231 + 20746t. \end{cases} \quad t = 0, \pm 1, \pm 2, \cdots.$$

4. 解：这是一个三元一次联立方程式，我们可以使用消

无法消去其中的一个未知数，就得到二元一次方程了．将第一式乘以 2 再加上第二式就可以消去 z 而得到

$$13x + 13y = 52,$$

即

$$x + y = 4.$$

容易看出 $x = 4$, $y = 0$ 是上面方程的一组解．它的全部解是

$$\begin{cases} x = 4 - t, \\ y = t. \end{cases} \quad t = 0, \pm 1, \pm 2, \cdots.$$

把这个解代入原方程的第二式，得到

$$3(4 - t) - t - 4z = 4,$$

即

$$z = 2 - t, \quad t = 0, \pm 1, \cdots.$$

现在要求出所有正整数解．令 $x > 0$, $y > 0$, $z > 0$, 就有

$$4 - t > 0, \quad t > 0, \quad 2 - t > 0,$$

即 $0 < t < 2$. 所以只能取 $t = 1$. 把它代入解中，得到原方程组的唯一的一组正整数解是 $x = 3$, $y = 1$, $z = 1$.

5. 解：设以 x, y, z 分别代表取一分、二分、五分硬币的数目，因此得到下面的方程

$$x + 2y + 5z = 18,$$
$$x + y + z = 10.$$

二式相减得到 $y + 4z = 8$.

我们要求出上方程的非负整数解．今先解

$$u + 4v = 1.$$

由于 $4 = 3 + 1$, 得到 $1 = -3 + 4$. 所以 $u = -3$, $v = 1$ 是 $u + 4v = 1$ 的一组整数解．因而

$$y = 8 \times (-3) = -24, \quad z = 8 \times 1 = 8$$

是 $y + 4z = 8$ 的一组整数解，它的全部整数解是

$$y = -24 - 4t, \quad z = 8 + t, \quad t = 0, \pm 1, \pm 2, \cdots.$$

所以

$$x = 10 - y - z = 26 + 3t.$$

按题意必须 $x \geqslant 0$, $y \geqslant 0$, $z \geqslant 0$. 由 $x = 26 + 3t \geqslant 0$ 得到 $t \geqslant -\frac{26}{3}$; 由 $y = -24 - 4t \geqslant 0$ 得到 $t \leqslant -6$; 由 $z = 8 + t \geqslant 0$ 得到 $t \geqslant -8$. 因此 $-8 \leqslant t \leqslant -6$(取 $t = -8, -7, -6$) 对应的三组解是

$$\begin{cases} x = 2 \\ y = 8 \\ z = 0, \end{cases} \quad \begin{cases} x = 5 \\ y = 4 \\ z = 1, \end{cases} \quad \begin{cases} x = 8 \\ y = 0 \\ z = 2. \end{cases}$$

所以有三种不同的取法，即上面的三组解.

6. 解：以 x, y 分别表示裁剪成大人和小孩衣服的件数，则有方程

$$7.2x + 3y = 75,$$

即

$$12x + 5y = 125.$$

现求它的非负整数解. 今先解

$$12u + 5v = 1.$$

由于 $12 = 2 \times 5 + 2$, $5 = 2 \times 2 + 1$, 而得

$$\begin{aligned} 1 &= 5 - 2 \times 2 = 5 - 2 \times (12 - 2 \times 5) \\ &= 12 \times (-2) + 5 \times 5, \end{aligned}$$

所以 $u = -2$, $v = 5$ 是 $12u + 5v = 1$ 的一组整数解. 因而 $x = 125 \times (-2) = -250$, $y = 125 \times 5 = 625$ 是 $12x + 5y = 125$ 的一组整数解. 它的全部整数解是 $x = -250 - 5t$, $y = 625 + 12t$, 即 $x = -5t$, $y = 25 + 12t$, $t = 0, \pm 1, \pm 2, \cdots$. 按题意要求 $x \geqslant 0$, $y \geqslant 0$. 由 $x = -5t \geqslant 0$ 得到 $t \leqslant 0$. 由 $y = 25 + 12t \geqslant 0$ 得到 $t \geqslant -\frac{25}{12}$. 故有

$$-\frac{25}{12} \leqslant t \leqslant 0.$$

分别取 $t = 0, -1, -2$，对应的三组解是

$$\begin{cases} x = 0 \\ y = 25, \end{cases} \quad \begin{cases} x = 5 \\ y = 13, \end{cases} \quad \begin{cases} x = 10 \\ y = 1. \end{cases}$$

7. 解：假设十位数是 x，个位数是 y，根据题意有

$$10x + y = 3xy.$$

等式两边同除以 x 得到

$$10 + \frac{y}{x} = 3y.$$

上式中由于 10 和 $3y$ 都是整数，所以 $\frac{y}{x}$ 也一定是整数．假设 $z = \frac{y}{x}$，则原方程变为

$$3y - z = 10.$$

容易看出 $y = 4$，$z = 2$ 是它的一组解． 它的全部整数解是

$$\begin{cases} y = 4 + t, \\ z = 2 + 3t, \end{cases} \quad t = 0, \pm 1, \pm 2, \cdots.$$

现在讨论 x 和 y 所应当满足的条件， 二位数必须满足 $0 \leqslant y \leqslant 9$，$1 \leqslant x \leqslant 9$．所以

$$z = \frac{y}{x} \geqslant 0.$$

即

$$2 + 3t \geqslant 0, \quad t \geqslant -\frac{2}{3}.$$

又 $y = xz \geqslant z$．所以

$$4 + t \geqslant 2 + 3t, \text{即 } t \leqslant 1.$$

因此 $-\frac{2}{3} \leqslant t \leqslant 1$，所以 t 只能取 0，1 二个值．将 $t = 0, 1$ 代入解中得到

$$t = 0 \text{ 时 } y = 4, \ z = 2, \ x = \frac{y}{z} = 2.$$

$$t = 1 \text{ 时 } y = 5,\ z = 5,\ x = \frac{y}{z} = 1.$$

所求的二位数是 24 和 15.

8. 证：证明分三步.

(i) 假如 R_1 和 R_2 是能够写成形状为 $ax + by$ 的二个整数，这里 a 和 b 是固定的正整数，x 和 y 是整数，则 $k_1R_1 + k_2R_2$（k_1，k_2 是整数）也可以写成 $ax + by$ 的形式. 这是因为假若

$$R_1 = ax_1 + by_1, \quad R_2 = ax_2 + by_2,$$

则

$$k_1R_1 + k_2R_2 = a(k_1x_1 + k_2x_2) + b(k_1y_1 + k_2y_2).$$

由于 $k_1x_1 + k_2x_2$ 和 $k_1y_1 + k_2y_2$ 都是整数，所以 $k_1R_1 + k_2R_2$ 也是形如 $ax + by$ 的数.

(ii) 由第一章的引理 4 可知，若 a 和 b 是正整数，且 $a > b$，则必存在 $q_1 > 0$，使得

$$a = bq_1 + r_1, \text{ 且 } 0 \leqslant r_1 < b.$$

同样由于 $b > r_1$，故存在 $q_2 > 0$，使得

$$b = r_1q_2 + r_2, \text{ 且 } 0 \leqslant r_2 < r_1.$$

这样继续下去，由于余数 r_1，r_2，$\cdots$ 逐次减小，所以经过有限步以后，最后终可使余数为 0. 因此我们有

$$\left.\begin{array}{ll} a \Rightarrow bq_1 + r_1, & 0 < r_1 < b; \\ b = r_1q_2 + r_2, & 0 < r_2 < r_1; \\ r_1 = r_2q_3 + r_3, & 0 < r_3 < r_2; \\ \cdots\cdots\cdots & \cdots\cdots; \\ r_{n-2} = r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1}; \end{array}\right\} \quad (1)$$

$$r_{n-1} = r_nq_{n+1},$$

最后一式的余数为 0. 由第一章的引理 8 可知：由 (1) 中的第一式有 $(a, b) = (b, r_1)$，由第二式有 $(b, r_1) = (r_1, r_2)$，由第三式有 $(r_1, r_2) = (r_2, r_3)$，以此类推，直到最后一式有

$(r_{n-1}, r_n) = r_n$. 所以有：

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = r_n,$$

即最后一个余数 r_n 就是 a 和 b 的最大公约数，这就是辗转相除法的原理. 现 a 和 b 互素，所以 $r_n = 1$.

(iii) 把 (1) 式写成：

$$\left.\begin{aligned} r_1 &= a - q_1 b, \\ r_2 &= b - q_2 r_1, \\ r_3 &= r_1 - q_3 r_2, \\ &\cdots\cdots\cdots \\ r_n &= r_{n-2} - q_n r_{n-1}. \end{aligned}\right\} \qquad (2)$$

这里 $q_1, \cdots, q_n$ 都是整数. 由(i)的讨论可知，由于 a 和 b 本身是形如 $ax + by$ 的数，故由 (2) 中的第一式，r_1 是形如 $ax + by$ 的数；又由第二式，b 和 r_1 是形如 $ax + by$ 的数，所以 r_2 是形如 $ax + by$ 的数；又由第三式，r_1 和 r_2 是形如 $ax + by$ 的数，所以 r_3 是形如 $ax + by$ 的数. 以此类推，最后由最末一式，由于 r_{n-2} 和 r_{n-1} 是形如 $ax + by$ 的数，所以 r_n 是形如 $ax + by$ 的数. 由 (ii) 的讨论已知 $r_n = 1$，因而必存在二个整数 x 和 y，使得 $ax + by = 1$.

9. 证：(i) 先证明 $\frac{z+y}{2}$ 和 $\frac{z-y}{2}$ 都是整数，并且

$$\left(\frac{z+y}{2}, \frac{z-y}{2}\right) = 1.$$

由于 x 是偶数，所以 x^2 是偶数，而由 $(x, y) = 1$ 可知 y 一定是奇数，于是 y^2 也是奇数，因此 $x^2 + y^2$ 是奇数，又 x, y, z 满足

$$x^2 + y^2 = z^2, \qquad (3)$$

故由 (3) 式可知 z^2 是奇数，于是 z 也是奇数. 由于 z 和 y 都是奇数，所以 $z + y$ 和 $z - y$ 都是偶数，因而证明了

$\frac{z+y}{2}$和$\frac{z-y}{2}$都是整数．假设

$$\left(\frac{z+y}{2}, \frac{z-y}{2}\right)=d,$$

则可以写成

$$\begin{cases}\dfrac{z+y}{2}=k_1d, \\ \dfrac{z-y}{2}=k_2d,\end{cases}$$

其中$(k_1, k_2)=1$，将上二式相减得到$y=(k_1-k_2)d$，所以$d|y$．又由(3)式得

$$x^2=z^2-y^2=(z+y)(z-y)=4k_1k_2d^2,$$

所以$d^2|x^2$，即$d|x$．因为d同时除尽x和y，故有$d|(x, y)$．但已知$(x, y)=1$，所以$d=1$．因而证明了

$$\left(\frac{z+y}{2}, \frac{z-y}{2}\right)=1.$$

(ii) 把(3)式改写成

$$x^2=(z+y)(z-y), \tag{4}$$

即

$$\left(\frac{x}{2}\right)^2=\left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right).$$

由于$2|x$，所以上式左端是一个平方数，而由(i)的讨论可知右端的二个因数互素，因此这二个因数本身一定都是平方数．令

$$\begin{aligned}\frac{z+y}{2}&=a^2, \\ \frac{z-y}{2}&=b^2,\end{aligned} \tag{5}$$

则由于x, y, z都是正整数，所以$a>b>0$．并且由上式可知$(a^2, b^2)=1$，因而$(a, b)=1$．把(5)中的二个式子相

加和相减就分别得到 $z = a^2 + b^2$, $y = a^2 - b^2$. 再由 (4) 和 (5) 得到 $x^2 = (z + y)(z - y) = 4a^2b^2$, 因而 $x = 2ab$. 又由于 z 是奇数，而 $z = a^2 + b^2$, 所以 a 和 b 中必定有一个是奇数，另一个是偶数. 于是 $a + b$ 是奇数，所以 $2\nmid(a + b)$, 因此 a 和 b 满足题中提出的所有条件.

10. 证：设 x, y 是直角边长，z 是斜边的长且 $z - x = 1$. 由勾股定理可知

$$x^2 + y^2 = z^2. \tag{6}$$

由于 $z - x = 1$, 所以 $(x, z) = 1$. 于是由 (6) 式必有 $(x, y) = 1$. 按本章的讨论可知满足 (6) 的解 x 和 y 必定有一个是奇数，另一个是偶数. 而 z 是奇数. 由于 $z - x = 1$, 所以 x 必为偶数，即 $2|x$, 因此 (6) 的解满足定理 2 的所有条件，由定理 2 得到三个边长的公式可表示成

$$x = 2ab, \quad y = a^2 - b^2, \quad z = a^2 + b^2. \tag{7}$$

这里 a 和 b 是正整数，$a > b$, $(a, b) = 1$, $2\nmid(a + b)$. 由于 $z - x = 1$, 由 (7) 得到 $a^2 + b^2 - 2ab = 1$. 所以 $(a - b)^2 = 1$, 因 $a > b$, 于是 $a - b = 1$, 即 $a = 1 + b$. 把它代入 (7) 式，得到边长公式为

$$x = 2ab = 2(1 + b)b = 2b^2 + 2b,$$
$$y = a^2 - b^2 = (1 + b)^2 - b^2 = 2b + 1,$$
$$z = a^2 + b^2 = (1 + b)^2 + b^2 = 2b^2 + 2b + 1,$$

其中 b 是任意正整数.

11. 证：将方程两边平方得到

$$\begin{aligned} z^4 &= (x^4 - 4y^4)^2 \\ &= x^8 - 8x^4y^4 + 16y^8 \\ &= (x^8 + 8x^4y^4 + 16y^8) - 16x^4y^4 \\ &= (x^4 + 4y^4)^2 - (2xy)^4, \end{aligned}$$

即

$$(2xy)^4 + z^4 = (x^4 + 4y^4)^2.$$

由此可以看到：如果 x_0，y_0，z_0 是方程 $x^4-4y^4=z^2$ 的一个正整数解，那末 $2x_0y_0$，z_0，$x_0^4+4y_0^4$ 就是方程 $x^4+y^4=z^2$ 的正整数解．从引理 3 的证明中已经知道 $x^4+y^4=z^2$ 没有正整数解，所以 $x^4-4y^4=z^2$ 不可能有正整数解．

第四章

1．解：从“八一”到国庆共有 61 天，由于

$$61\equiv 5 \pmod 7,$$

及“八一”是星期二，所以国庆是星期日．

2．

(i) 解：由于

$4568\equiv 4+5+6+8\equiv 5 \pmod 9$，

$7391\equiv 7+3+1\equiv 2 \pmod 9$，

$30746529\equiv 3+7+4+6+5+2\equiv 0 \pmod 9$，

而

$$2\times 5\not\equiv 0 \pmod 9,$$

所以原式计算有错误．

(ii) 解：由于

$2368\equiv 2+3+6+8\equiv 1 \pmod 9$，

$846\equiv 8+4+6\equiv 0 \pmod 9$，

$2003328\equiv 2+3+3+2+8\equiv 0 \pmod 9$，

而

$$1\times 0\equiv 0 \pmod 9,$$

所以原式计算有可能是正确的．

(iii) 解：由于

$16\equiv 7 \pmod 9$，　　$937\equiv 3+7\equiv 1 \pmod 9$，

$1559\equiv 1+5+5\equiv 2 \pmod 9$，

$23373528\equiv 2+3+3+7+3+5+2+8$

$$\equiv 6 \pmod 9,$$

而

$$7 \times 1 \times 2 \not\equiv 6 \pmod 9,$$

所以原式计算是错误的.

(iv) 解：由于

$$17 \equiv -1 \pmod 9,$$

所以由引理 7 得到

$$17^4 \equiv (-1)^4 \equiv 1 \pmod 9,$$

而

$$83521 \equiv 8 + 3 + 5 + 2 + 1 \equiv 1 \pmod 9,$$

所以原式有可能是正确的.

(v) 解：此式就是 $3748 \times 6236 = 23372428$，所以仍可用弃九法验算. 由于

$$3748 \equiv 3 + 7 + 4 + 8 \equiv 4 \pmod 9,$$

$$6236 \equiv 6 + 2 + 3 + 6 \equiv 8 \pmod 9,$$

$$23372428 \equiv 2 + 3 + 3 + 7 + 2 + 4 + 2 + 8 \equiv 4 \pmod 9,$$

而

$$4 \times 8 \not\equiv 4 \pmod 9,$$

所以原式计算是错误的.

3. 证：一次同余式

$$ax + b \equiv 0 \pmod m, a \not\equiv 0 \pmod m \qquad (1)$$

有解的条件等价于不定方程

$$ax - my = -b \qquad (2)$$

有解. 令 $a = a'd$, $m = m'd$, 则 $(a', m') = 1$. 又因 $(a, m) | b$, 故可取 $b = b'd$, (2) 式就成为

$$a'x - m'y = -b'. \qquad (3)$$

由于 $(a', m') = 1$，及第三章引理 2 可知 (3) 式有解，设它的解是 x_0, y_0, 所以(1)式在 $(a, m) | b$ 时有解. 又由第三章定理 1 知 (3) 式的全部整数解中的 x 可以表示成

$$x = x_0 + m't, \quad t = 0, \pm 1, \pm 2, \cdots,$$

其中 $m' = \frac{m}{d}$, 因此 (1) 式的解可以写成

$$x \equiv x_0 + k \cdot \frac{m}{d} \pmod{m}, \quad k = 0, 1, \cdots, d-1.$$

由于 $k = 0, 1, \cdots, d-1$ 时，$x_0 + k \cdot \frac{m}{d}$ 对模 m 两两不同余，所以 (1) 式有 d 个解.

4.

(i) 解：由于

$$(258, 348) = 6,$$

而 $6 \nmid 131$，所以由引理 11 知同余式无解.

(ii) 解：由于

$$29 = 9 \times 3 + 2, \quad 3 = 2 + 1,$$

所以

$$1 = 3 - 2 = 3 - (29 - 9 \times 3) = 10 \times 3 - 29,$$

即

$$3 \times 10 \equiv 1 \pmod{29}.$$

由原式得到

$$3 \times 10x \equiv 10 \times 10 \pmod{29},$$

所以

$$x \equiv 100 \equiv 13 \pmod{29}.$$

(iii) 解：由于

$$111 = 2 \times 47 + 17, \quad 47 = 2 \times 17 + 13,$$
$$17 = 13 + 4, \quad 13 = 3 \times 4 + 1,$$

所以

$$\begin{aligned} 1 &= 13 - 3 \times 4 = 13 - 3 \times (17 - 13) \\ &= 4 \times 13 - 3 \times 17 = 4 \times (47 - 2 \times 17) - 3 \times 17 \\ &= 4 \times 47 - 11 \times 17 = 4 \times 47 - 11 \times (111 \end{aligned}$$

$$-2\times 47)=26\times 47-11\times 111,$$

即

$$26\times 47\equiv 1 \pmod{111}.$$

由原式

$$26\times 47x\equiv 26\times 89 \pmod{111},$$

所以

$$x\equiv 26\times 89\equiv 94 \pmod{111}.$$

(iv) 解：由于

$(660, 1385)=5$，而 $5|595$，所以由习题 3 知上式有五个解．今先解

$$132x\equiv 119 \pmod{277}.$$

由于

$$277=2\times 132+13,\quad 132=10\times 13+2,$$

$$13=6\times 2+1,$$

所以

$$1=13-6\times 2=13-6\times(132-10\times 13)$$

$$=61\times 13-6\times 132=61\times(277-2$$

$$\times 132)-6\times 132=61\times 277-128\times 132,$$

即

$$-128\times 132\equiv 1 \pmod{277}.$$

由原式

$$-128\times 132x\equiv -128\times 119 \pmod{277},$$

所以

$$x\equiv -128\times 119\equiv 3 \pmod{277}.$$

原同余式的五个解是

$$x\equiv 3 \pmod{1385},$$

$$x\equiv 280 \pmod{1385},$$

$$x\equiv 557 \pmod{1385},$$

$$x \equiv 834 \pmod{1385},$$
$$x \equiv 1111 \pmod{1385}.$$

5.

(i) 解：由孙子定理知道

$$b_1 = 3, \quad b_2 = 5, \quad m_1 = 7, \quad m_2 = 11,$$
$$m = m_1 \cdot m_2 = 7 \times 11 = 77,$$
$$M_1 = \frac{77}{7} = 11, \quad M_2 = \frac{77}{11} = 7.$$

由 $11M_1' \equiv 1 \pmod{7}$，得 $M_1' = 2$.

由 $7M_2' \equiv 1 \pmod{11}$，得 $M_2' = 8$.

所以解为

$$x \equiv 3 \times 11 \times 2 + 5 \times 7 \times 8$$
$$\equiv 346 \equiv 38 \pmod{77}.$$

(ii) 解：这里的模两两互素，可用孙子定理.

$$b_1 = 2, \quad b_2 = 5, \quad b_3 = 4,$$
$$m_1 = 11, \quad m_2 = 7, \quad m_3 = 5,$$
$$m = m_1 \cdot m_2 \cdot m_3 = 11 \times 7 \times 5 = 385,$$
$$M_1 = \frac{385}{11} = 35, \quad M_2 = \frac{385}{7} = 55,$$
$$M_3 = \frac{385}{5} = 77.$$

由

$$35M_1' \equiv 1 \pmod{11},$$

即

$$(11 \times 3 + 2)M_1' \equiv 1 \pmod{11},$$

所以

$$2M_1' \equiv 1 \pmod{11},$$

得到

$$M_1' = -5.$$

同样由

$$55M_2' \equiv 1 \pmod{7}, \quad \text{即 } 6M_2' \equiv 1 \pmod{7},$$

得

$$M_2' = -1.$$

由

$$77M_3' \equiv 1 \pmod{5}, \quad \text{即 } 2M_3' \equiv 1 \pmod{5},$$

得

$$M_3' = 3.$$

由孙子定理得到解为

$$x \equiv 2 \times 35 \times (-5) + 5 \times 55 \times (-1) + 4 \times 77 \times 3 \equiv 299 \pmod{385}.$$

(iii) 解：由第二式和第三式可分别得到

$$x \equiv 3 \pmod{5}, \quad x \equiv 5 \pmod{9}.$$

由第一式与上二式组成方程组就可用孙子定理求解.

$$b_1 = 1, \quad b_2 = 3, \quad b_3 = 5,$$

$$m_1 = 7, \quad m_2 = 5, \quad m_3 = 9,$$

$$m = m_1 \cdot m_2 \cdot m_3 = 7 \times 5 \times 9 = 315,$$

$$M_1 = \frac{315}{7} = 45, \quad M_2 = \frac{315}{5} = 63, \quad M_3 = \frac{315}{9} = 35.$$

由 $45M_1' \equiv 1 \pmod{7}$，得 $M_1' = -2$.

由 $63M_2' \equiv 1 \pmod{5}$，得 $M_2' = 2$.

由 $35M_3' \equiv 1 \pmod{9}$，得 $M_3' = -1$.

所以

$$x \equiv 1 \times 45 \times (-2) + 3 \times 63 \times 2 + 5 \times 35 \times (-1) \equiv 113 \pmod{315}.$$

6.

(i) 解：设本数为 x，则按题意有

$$\begin{cases} x \equiv 1 \pmod{7}, \\ x \equiv 2 \pmod{8}, \\ x \equiv 4 \pmod{9}. \end{cases}$$

这里 $b_1 = 1, \quad b_2 = 2, \quad b_3 = 4,$

$$m_1=7,\quad m_2=8,\quad m_3=9,$$

$$m=7\times 8\times 9=504,$$

$$M_1=\frac{504}{7}=72,\quad M_2=\frac{504}{8}=63,\quad M_3=\frac{504}{9}=56.$$

由 $72M_1'\equiv 1 \pmod 7$，得 $M_1'=4$.

由 $63M_2'\equiv 1 \pmod 8$，得 $M_2'=-1$.

由 $56M_3'\equiv 1 \pmod 9$，得 $M_3'=-4$.

所以

$$x\equiv 1\times 72\times 4+2\times 63\times(-1)+4\times 56\times(-4)\equiv -734\equiv 274 \pmod{504}.$$

(ii) 解：设本数为 x，按题意有

$$\begin{cases} x\equiv 1 \pmod 2,\\ x\equiv 2 \pmod 5,\\ x\equiv 3 \pmod 7,\\ x\equiv 5 \pmod 9.\end{cases}$$

这里 $b_1=1,\quad b_2=2,\quad b_3=3,\quad b_4=5,$

$$m_1=2,\quad m_2=5,\quad m_3=7,\quad m_4=9,$$

$$m=m_1\cdot m_2\cdot m_3\cdot m_4=2\times 5\times 7\times 9=630,$$

$$M_1=\frac{630}{2}=315,\qquad M_2=\frac{630}{5}=126,$$

$$M_3=\frac{630}{7}=90,\qquad M_4=\frac{630}{9}=70.$$

由 $315M_1'\equiv 1 \pmod 2$，得 $M_1'=1$.

由 $126M_2'\equiv 1 \pmod 5$，得 $M_2'=1$.

由 $90M_3'\equiv 1 \pmod 7$，得 $M_3'=-1$.

由 $70M_4'\equiv 1 \pmod 9$，得 $M_4'=4$.

所以

$$x\equiv 315+2\times 126+3\times 90\times(-1)+5\times 70\times 4\equiv 1697\equiv 437 \pmod{630}.$$

(iii) 解：设本数为 x，按题意有

$$\begin{cases} x \equiv 3 \pmod{11}, \\ x \equiv 2 \pmod{72}, \\ x \equiv 1 \pmod{13}. \end{cases}$$

这里 $b_1 = 3,\quad b_2 = 2,\quad b_3 = 1,$

$$m_1 = 11,\quad m_2 = 72,\quad m_3 = 13,$$

$$m = m_1 \cdot m_2 \cdot m_3 = 11 \times 72 \times 13 = 10296,$$

$$M_1 = \frac{10296}{11} = 936,\qquad M_2 = \frac{10296}{72} = 143,$$

$$M_3 = \frac{10296}{13} = 792.$$

由 $936M_1' \equiv 1 \pmod{11}$，得 $M_1' = 1$.

由 $143M_2' \equiv 1 \pmod{72}$，得 $M_2' = -1$.

由 $792M_3' \equiv 1 \pmod{13}$，得 $M_3' = -1$.

所以

$$x \equiv 3 \times 936 + 2 \times 143 \times (-1) + 1 \times 792 \times (-1) \equiv 1730 \pmod{10296}.$$

7. 证：由 $x \equiv a(\bmod\{m_1, m_2\})$ 可知

$$\{m_1, m_2\} \mid (x - a).$$

而 $m_1 \mid \{m_1, m_2\}$，$m_2 \mid \{m_1, m_2\}$，所以由第一章引理 2 知

$$m_1 \mid (x - a),\quad m_2 \mid (x - a),$$

即

$$x \equiv a \pmod{m_1},\quad x \equiv a \pmod{m_2}.$$

这就证明了 $x \equiv a \pmod{\{m_1, m_2\}}$ 是同余式组 $x \equiv a \pmod{m_1}$，$x \equiv a \pmod{m_2}$ 的解。

反之，设 x_0 是满足 $x \equiv a \pmod{m_1}$，$x \equiv a \pmod{m_2}$ 的整数，则由同余的定义知，

$$m_1 \mid (x_0 - a),\quad m_2 \mid (x_0 - a),$$

因此由第一章引理 9 知 $\{m_1, m_2\} \mid (x_0 - a)$，即

$$x_0 \equiv a \pmod{\{m_1, m_2\}}.$$

所以 $x \equiv a \pmod{\{m_1, m_2\}}$ 是同余式组 $x \equiv a \pmod{m_1}$, $x \equiv a \pmod{m_2}$ 的全部解。

8.

(i) 证：令 $\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases}$ (4)

由 (4) 式知

$$x = b_1 + m_1 t_1,$$
$$x = b_2 + m_2 t_2.$$

这里 t_1, t_2 是整数，(4) 式有解就是存在整数 t_1, t_2 使得

$$b_1 + m_1 t_1 = b_2 + m_2 t_2,$$

即

$$m_2 t_2 - m_1 t_1 = b_1 - b_2.$$

令 $m_1 = m_1' d$, $m_2 = m_2' d$, 则 $(m_1', m_2') = 1$. 又设

$$c = \frac{b_1 - b_2}{d},$$

上式就成

$$m_2' t_2 - m_1' t_1 = c.$$

当 $d \mid (b_1 - b_2)$ 时，c 是整数，又 $(m_1', m_2') = 1$. 由第三章引理 2 知上式有解，因此 (4) 式在 $d \mid (b_1 - b_2)$ 时有解. 若 x_0 是满足 (4) 式的一个整数，则

$$x_0 \equiv b_1 \pmod{m_1}, \quad x_0 \equiv b_2 \pmod{m_2}.$$

所以同余式组 (4) 与同余式组

$$\begin{cases} x \equiv x_0 \pmod{m_1} \\ x \equiv x_0 \pmod{m_2} \end{cases}$$

的解完全相同. 由习题 7 知上同余式组的全部解是

$$x \equiv x_0 \pmod{\{m_1, m_2\}}.$$

因而 (4) 式的全部解是

$$x \equiv x_0 \pmod{\{m_1, m_2\}}.$$

注：此题的结果可以推广到多个同余式的情形．即同余式组

$$x \equiv b_i \pmod{m_i}, \quad i = 1, 2, \cdots, k$$

在 $(m_i, m_j) | (b_i - b_j)$，$i, j = 1, 2, \cdots, k$ 时必定有解．若 x_0 是满足上同余式组的一个整数，则它的全部解是

$$x \equiv x_0 \pmod{\{m_1, m_2, \cdots, m_k\}}.$$

(ii) 证：令 $x \equiv b_i \pmod{m_i}$，$i = 1, 2, \cdots k$　　(5)

$$x \equiv b_i \pmod{n_i}, \quad i = 1, 2, \cdots k \qquad (6)$$

由 (i) 可知同余式组 (5) 的全部解是

$$x \equiv x_0 \pmod{\{m_1, m_2, \cdots, m_k\}}.$$

这里 x_0 是满足 (5) 式的一个整数，所以有

$$x_0 \equiv b_i \pmod{m_i}, \quad i = 1, 2, \cdots, k.$$

由于 $n_i | m_i$，因此有

$$x_0 \equiv b_i \pmod{n_i}, \quad i = 1, 2, \cdots, k.$$

即 x_0 也是满足 (6) 式的一个整数．由 (i) 可知 (6) 式的全部解是

$$x \equiv x_0 \pmod{\{n_1, n_2, \cdots, n_k\}}.$$

由于 $\{n_1, n_2, \cdots, n_k\} = \{m_1, m_2, \cdots, m_k\}$，所以同余式组 (5) 和 (6) 的解完全相同．

注：(i) 指出了当模不两两互素时，如何判断同余式组 (5) 是否有解．(ii) 指明了在 (5) 式有解的情况下可以化为对 (6) 式的求解．而同余式组 (6) 的模是两两互素的，可以用孙子定理求解．因此本题解决了模不两两互素时同余式组的求解问题．

9.

(i) 解：由于 $(7, 9) = 1$，$(7, 15) = 1$，$(9, 15) = 3$，$11 - 5 = 6$，而 $3 | (11 - 5)$，由习题 8(i,ii) 知同余式组有解且与

$$\begin{cases} x \equiv 2 \pmod 7 \\ x \equiv 5 \pmod 9 \\ x \equiv 11 \equiv 1 \pmod 5 \end{cases}$$

有相同的解．用孙子定理解上式

$$b_1 = 2, \quad b_2 = 5, \quad b_3 = 1,$$

$$m_1 = 7, \quad m_2 = 9, \quad m_3 = 5,$$

$$m = m_1 \cdot m_2 \cdot m_3 = 7 \times 9 \times 5 = 315,$$

$$M_1 = \frac{315}{7} = 45, \quad M_2 = \frac{315}{9} = 35, \quad M_3 = \frac{315}{5} = 63.$$

由 $45M_1' \equiv 1 \pmod 7$，得 $M_1' = -2$.

由 $35M_2' \equiv 1 \pmod 9$，得 $M_2' = -1$.

由 $63M_3' \equiv 1 \pmod 5$，得 $M_3' = 2$.

所以解为

$$x \equiv 2 \times 45 \times (-2) + 5 \times 35 \times (-1) + 1 \times 63 \times 2 \equiv -229 \equiv 86 \pmod{315}.$$

(ii) 解：设总数是 x，按题意有

$$\begin{cases} x \equiv 0 \pmod 5, \\ x \equiv 10 \pmod{715}, \\ x \equiv 140 \pmod{247}, \\ x \equiv 245 \pmod{391}, \\ x \equiv 109 \pmod{187}. \end{cases}$$

先检验是否有解．由于 $715 = 5 \times 11 \times 13$, $247 = 13 \times 19$, $391 = 17 \times 23$, $187 = 11 \times 17$，所以 $(5, 715) = 5$，而 $5 \mid (10-0)$; $(715, 247) = 13$，而 $13 \mid (140-10)$; $(715, 187) = 11$，而 $11 \mid (109-10)$; $(391, 187) = 17$，而 $17 \mid (245-109)$; 因此由习题 8 (i) 知同余式组有解．由习题 8 (ii) 适当选择模，使原同余式组与下面的同余式组有相同的解

$$\begin{cases} x \equiv 0 \pmod{5}, \\ x \equiv 10 \pmod{11 \times 13}, \\ x \equiv 140 \equiv 7 \pmod{19}, \\ x \equiv 245 \equiv 15 \pmod{23}, \\ x \equiv 109 \equiv 7 \pmod{17}. \end{cases}$$

上同余式组的模两两互素，可用孙子定理求解.

$$b_1 = 0,\quad b_2 = 10,\quad b_3 = 7,\quad b_4 = 15,\quad b_5 = 7,$$

$$m_1 = 5,\quad m_2 = 11 \times 13,\quad m_3 = 19,\quad m_4 = 23,$$

$$m_5 = 17,\quad m = 5 \times 11 \times 13 \times 19 \times 23 \times 17$$

$$= 5311735,$$

$$M_1 = \frac{5311735}{5} = 1062347,$$

$$M_2 = \frac{5311735}{11 \times 13} = 37145,$$

$$M_3 = \frac{5311735}{19} = 279565,$$

$$M_4 = \frac{5311735}{23} = 230945,$$

$$M_5 = \frac{5311735}{17} = 312455.$$

由 $1062347M_1' \equiv 2M_1' \equiv 1 \pmod{5}$，得 $M_1' = 3$.

由 $37145M_2' \equiv 108M_2' \equiv 1 \pmod{11 \times 13}$

又 $11 \times 13 = 143$

因为

$$143 = 108 + 35,\quad 108 = 3 \times 35 + 3,$$

$$35 = 11 \times 3 + 2,\quad 3 = 2 + 1,$$

所以

$$1 = 3 - 2 = 3 - (35 - 11 \times 3) = 12 \times 3 - 35$$

$$= 12 \times (108 - 3 \times 35) - 35$$

$$= 12 \times 108 - 37 \times 35$$

$$= 12 \times 108 - 37 \times (143 - 108)$$
$$= 49 \times 108 - 37 \times 143.$$

即

$$108 \times 49 \equiv 1 \pmod{143}, \text{得 } M_2' = 49.$$

由 $279565M_3' \equiv 18M_3' \equiv 1 \pmod{19}$，得 $M_3' = -1$.

由 $230945M_4' \equiv 2M_4' \equiv 1 \pmod{23}$，得 $M_4' = -11$.

由 $312455M_5' \equiv 12M_5' \equiv 1 \pmod{17}$，得 $M_5' = -7$.

最后得出解是

$$x \equiv 10 \times 37145 \times 49 + 7 \times 279565 \times (-1)$$
$$+ 15 \times 230945 \times (-11) + 7 \times 312455$$
$$\times (-7) \equiv 18201050 - 1956955 - 38105925$$
$$- 15310295 \equiv -37172125$$
$$\equiv 10020 \pmod{5311735}.$$

答：总数最小为 10020.

10. 解：设甲、乙两港距离 x 公里. 第二只轮船 18 小时走的距离是 $240 \times \frac{18}{24} = 180$ 公里，第三只轮船 8 小时走的距离是 $180 \times \frac{8}{24} = 60$ 公里. 按题意有

$$\begin{cases} x \equiv 0 \pmod{300}, \\ x \equiv 180 \pmod{240}, \\ x \equiv 60 \pmod{180}. \end{cases}$$

由于

$$(300, 240) = 60, \text{而 } 60 \mid (180 - 0);$$
$$(300, 180) = 60, \text{而 } 60 \mid (60 - 0);$$
$$(240, 180) = 60, \text{而 } 60 \mid (180 - 60);$$

所以同余式组有解. 因

$$300 = 2^2 \times 3 \times 5^2,$$
$$240 = 2^4 \times 3 \times 5,$$

$$180 = 2^4 \times 3^2 \times 5,$$

所以原同余式组与

$$\begin{cases} x \equiv 0 \pmod{5^2} \\ x \equiv 180 \equiv 4 \pmod{2^4} \\ x \equiv 60 \equiv 6 \pmod{3^2} \end{cases}$$

有相同的解．用孙子定理求解．此处

$$b_1 = 0, \quad b_2 = 4, \quad b_3 = 6,$$

$$m_1 = 5^2, \quad m_2 = 2^4, \quad m_3 = 3^2,$$

$$m = 5^2 \times 2^4 \times 3^2 = 3600,$$

$$M_1 = \frac{3600}{5^2} = 144, \qquad M_2 = \frac{3600}{2^4} = 225,$$

$$M_3 = \frac{3600}{9} = 400.$$

由 $144M_1' \equiv 1 \pmod{5^2}$，即 $19M_1' \equiv 1 \pmod{5^2}$，得 $M_1' = 4$．
由 $225M_2' \equiv 1 \pmod{2^4}$，即 $M_2' \equiv 1 \pmod{2^4}$，得 $M_2' = 1$．
由 $400M_3' \equiv 1 \pmod{3^2}$，即 $4M_3' \equiv 1 \pmod{9}$，得 $M_3' = -2$．
所以

$$x \equiv 4 \times 225 \times 1 + 6 \times 400 \times (-2)$$
$$\equiv -3900 \equiv 3300 \pmod{3600}.$$

由于甲，乙两港距离不超过 5000 公里，所以实际距离为 3300 公里．

又

$$\frac{3300}{300} = 11.$$

$$\frac{3300}{240} = 13\frac{18}{24}.$$

$$\frac{3300}{180} = 18\frac{6}{18}.$$

答：甲，乙两港相距 3300 公里．第一只轮船走 11 天，第二只轮船走 13 天 18 小时，第三只轮船走 18 天 8 小时．